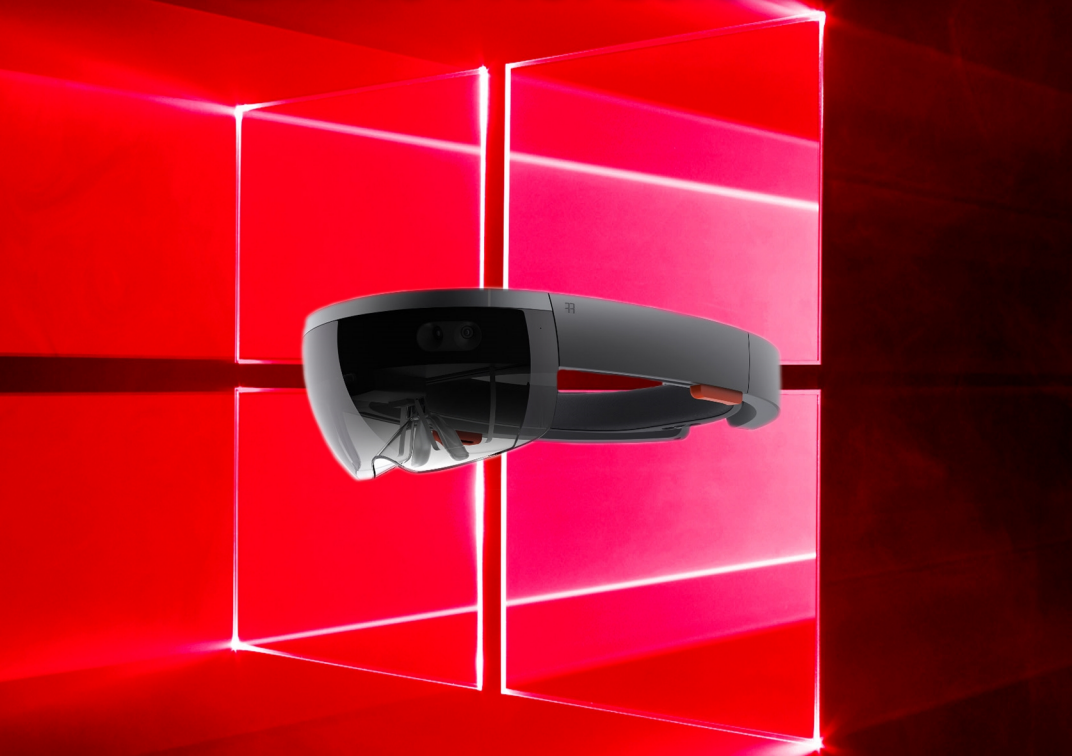
Nicolae Zărnescu

WINDOWS 10
PENTRU PROFESIONIȘTI



Editura Hoffman
2016

În memoria unchiului meu, Alexandru Teodorescu,
coordonatorul volumului „Sistemul Felix C-256 – Limbajul ASSIRIS”,
Ed. Academiei R.S.R., 1974

Nicolae Zărnescu

WINDOWS 10
pentru profesioniști

Editura Hoffman
2016

Descrierea CIP a Bibliotecii Naționale a României
ZĂRNESCU, NICOLAE
Windows 10 pentru profesioniști / Nicolae Zărnescu. – Caracal: Editura Hoffman, 2016
Conține bibliografie
Index
ISBN 978-606-778-020-8

004.451 WINDOWS 10

Bibliografie

- Revista CHIP nr. 9/2015
- Nicolae Zărnescu – *WINDOWS 10 GHID PRACTIC*
- Rob Tidrow, Jim Boyce, Jeffrey R. Shapiro - *WINDOWS 10 BIBLE*
- Microsoft Press – *INTRODUCING WINDOWS 10 FOR IT PROFESSIONALS*
- Microsoft Virtual Academy – *GETTING STARTED WITH WINDOWS 10 FOR IT PROS*
- Lynda.com – *WINDOWS 10 FOR SMALL BUSINESSES*
- Lynda.com – *WINDOWS 10 FUNDAMENTALS FOR IT PROS*

Tehnoredactare computerizată: Nicolae Zărnescu

©2016, Nicolae Zărnescu. Toate drepturile rezervate.
©Editura Hoffman, 2016, pentru prezenta ediție.
Orice reproducere, totală sau parțială, a acestei lucrări, fără acordul scris al editorului, este strict interzisă și se pedepsește conform Legii dreptului de autor.

www.EdituraHoffman.com
Tel./fax: 0249 460 218
0740 984 910

Noutăți pentru profesioniști

Considerații generale

Principala problemă cu care se confruntă specialiștii IT este asigurarea securității informatice a instituției, atunci când angajații utilizează *echipamente aduse de acasă* (smartphone-uri, tablete, laptopuri sau chiar PC-uri), fenomen cunoscut sub denumirea de „*consumerization of IT*" sau *BYOD (Bring Your Own Device)*. Specialiștii IT au posibilitatea să aleagă diverse soluții, care să asigure securitatea rețelei locale, atunci când aceasta este accesată prin intermediul unor astfel de echipamente.

Securitate sporită cu Windows 10

Windows 8 a introdus soluții sporite de securitate, care au fost îmbunătățite în Windows 8.1 și Windows 10.

Pentru echipamentele cu hardware avansat, Windows 10 a introdus mai multe soluții importante privind autentificarea acestora:

Windows Hello Prin această soluție se utilizează *autentificarea biometrică* (recunoașterea amprentei, recunoașterea facială și scanarea irisului). *Windows Hello* necesită, pentru recunoașterea facială, o *cameră web cu vedere în infraroșu* (similară cu tehnologia utilizată de senzorul *Xbox Kinect*), pentru a elimina posibilitatea recunoașterii false, pe baza unei fotografii, iar pentru recunoașterea amprentei echipamentul trebuie dotat cu un dispozitiv hardware special.

Microsoft Passport Această a doua soluție este bazată pe noul *API (Application Programming Interface)*, care lucrează în tandem cu autentificarea biometrică. Pașaportul le permite specialiștilor IT alegerea unei alternative de securitate la vechea metodă bazată pe parole, eliminând astfel cele mai comune breșe de securitate, ce le permiteau hackerilor să introducă *rootkit*uri și *malware*-uri. Pe echipamentele dotate cu *UEFI (Unified Extensible Firmware Interface)*, prin procedura *Secure Boot,* se verifică dacă aplicațiile de startup și încărcătorul sistemului de operare au o *semnătură* validată prin hardware, împiedicând bootarea neautorizată. După ce încărcătorul preia controlul sistemului de operare, sunt disponibile alte două opțiuni de securitate:

Trusted boot Prin această procedură se verifică *nucleul* (kernel), *fișierele sistem*, *driverele de boot* și chiar *aplicația antimalware*. Driverele *ELAM (Early Launch Antimalware)* sunt inițializate înaintea acestora și dau controlul aplicației antimalware înainte de bootare, blocând încercările de imixtiune din exterior în timpul procesului de încărcare a sistemului de operare.

Measured boot Pe echipamentele care includ *TPM (Trusted Platform Module)*, Windows 10 efectuează o serie de *măsurători* de integritate pe parcursul bootării sistemului de operare și memorează rezultatele în TPM. La următoarea pornire a sistemului de operare, *nucleul sistemului* și *driverele de boot* sunt măsurate și comparate cu *informațiile corecte, stocate pe un alt echipament*, care validează integritatea acestora, procedură numită *Remote Attestation* (atestare de la distanță).

După bootarea sistemului de operare, Windows 10 utilizează alte două soluții pentru blocarea malware-urilor:

Windows Defender Acesta este succesorul lui *Microsoft Security Essentials* și nu este mare consumator de resurse, actualizându-și, în mod regulat, semnăturile și motorul antimalware. Dacă veți instala altă aplicație antimalware, Windows Defender nu va mai asigura protecție în timp real, dar rămâne utilizabil în continuare.

Windows SmartScreen În acest caz se utilizează *tehnologiile bazate pe reputație* (application reputation-based technologies) pentru a proteja utilizatorii de atacurile malware, verificând fiecare aplicație înainte de instalarea acesteia și blocând aplicațiile cu grad ridicat de risc. *SmartScreen* asigură și protecția împotriva *site-urilor* care încearcă să fure *informații personale*, ca numele utilizatorului, parola sau date de pe cardurile cu care se face plata online.

Administratorii rețelei pot defini *politici de securitate* care *criptează* în mod automat informațiile esențiale: *aplicații*, *date*, *emailuri* sau *site*-uri *intranet*. Pentru o securitate sporită, administratorii pot crea o *listă* a aplicațiilor care pot *accesa datele criptate*, precum și o *listă* a aplicațiilor cu *acces interzis* sau care ar putea *muta datele în cloud*, de unde are putea fi accesate de hackeri.

Enterprise Data Protection Această facilitate este o variantă avansată a *RBDR (Remote Business Data Removal),* introdusă de Windows 8.1, prin care administratorii pot să *marcheze* și să *cripteze* datele aparținând *instituției*, pentru a le deosebi de datele personale ale *utilizatorului*. Când acesta își va schimba locul de muncă, nu va mai avea acces la datele confidențiale ale instituției.

Pervasive Device Encryption *Criptarea* dispozitivelor este disponibilă în toate versiunile de Windows 10, cu protecție suplimentară prin *BitLocker* în *Pro* și *Enterprise*. Dispozitivele care suportă facilitatea *InstantGo* (cunoscută anterior drept *Connected Standby*) sunt criptate în mod automat atunci când se utilizează un cont Microsoft. *BitLocker* suportă hard drive-uri care vin *precriptate* de producător, efectuând operații criptografice care scad nivelul de întrebuințare al procesoarelor și micșorează puterea consumată. Pe dispozitivele care *nu sunt precriptate*, BitLocker criptează datele *mai rapid decât sub Windows 7*, permițându-le administratorilor să aleagă *doar spațiul utilizat* de pe hard drive și nu tot hard drive-ul, *spațiul liber* fiind criptat doar *la prima utilizare*. În plus, i se poate permite unui utilizator standard, fără privilegii administrative, *să reseteze PIN-ul pentru BitLocker*. Pentru organizațiile care necesită un înalt nivel de securitate, versiunea *Enterprise* și hardware-ul *OEM* permit administratorilor să utilizeze *Device Guard*, pentru a bloca dispozitivele care încearcă să ruleze cod ce nu este de încredere (*untrusted code*). În această configurație, vor putea rula doar aplicațiile care sunt *semnate* printr-un *certificat emis de Microsoft*, inclusiv aplicațiile din Windows Store. Aplicațiile semnate sunt transmise apoi angajaților prin *Business Store.*

Implementare și administrare

Implementarea lui Windows 10 într-o organizație este *mai rapidă și mai ușoară decât în Windows 7*, datorită facilităților introduse de Windows 8.

Tradiționalul „*wipe and load*" (șterge și încarcă) este disponibil și pentru Windows 10. Acest proces presupune captarea datelor și a setărilor de la un dispozitiv existent, implementând o *imagine sistem utilizator*, adăugând *driverele* și *aplicațiile esențiale*, apoi *restaurând datele și setările* pe alt echipament cu performanțe identice.

O opțiune suplimentară este upgrade-ul *in-place*, prin care Windows gestionează procesul migrării aplicaților de la o imagine existentă la o nouă imagine standard. Acest proces este similar cu update-urile normale de Windows, dar este gestionat prin *System Center Configuration Manager (SCCM)* și *Microsoft Deployment Toolkit (MDT)*.

Prin *Refresh Your PC* se pot recupera datele, iar prin *Reset Your PC* se poate transfera dispozitivul unui nou utilizator, fără a dezvălui date personale ale instituției.

Virtualizare

Windows 10 include o platformă robustă de virtualizare numită *Client Hyper-V*, care utilizează același *hypervisor* ca și *Windows Server*, permițând crearea *mașinilor virtuale* capabile să ruleze versiuni pe 32 de biți sau pe 64 de biți ale sistemelor de operare client-server. *Evaluarea* și *depanarea* software-ului și a serviciilor se face mult mai ușor, fără a afecta activitatea utilizatorilor.

Clientul Hyper-V folosește infrastructura de securitate a lui Windows 10 și poate fi gestionat cu ușurință prin instrumentele IT existente, cum ar fi *System Center*. *Mașina virtuală (VM)* poate fi migrată de pe un PC desktop care rulează Windows 10 pe un mediu Hyper-V de pe Windows Server. Client Hyper-V necesită *Windows 10 Pro* sau *Windows 10 Enterprise* și un *hardware special*.

În combinație cu *Windows Server 2012 și 2016*, Windows 10 suportă o formă alternativă de virtualizare numită *Virtual Desktop Infrastructure (VDI)*, care poate fi setată foarte simplu, prin intermediul unui *wizard* (vrăjitor, magician).

Clientul *Remote Desktop* din Windows 10 le permite utilizatorilor să se conecteze la un *desktop virtual*, atât în rețele *LAN* (Local Area Network), cât și în rețele *WAN* (Wide Area Network). *Microsoft RemoteFX* include rularea aplicațiilor multimedia, afișarea graficii 3D, utilizarea perifericelor USB sau a dispozitivelor de intrare cu ecran tactil (touch screen).

Caracteristici cum ar fi *discurile cu profil utilizator* (user-profile disks) și *Fair Share* asigură o înaltă performanță și flexibilitate, cu suport pentru costuri de depozitare mai mici și sesiuni ajutând la reducerea costurilor VDI-urilor. Toate aceste beneficii sunt disponibile în diferite tipuri de desktop-uri VDI: *personal VM*, *pooled VM* sau *session-based desktops* (mașini virtuale personale, mașini virtuale reunite, desktop-uri bazate pe sesiune).

Cross-platform

Windows 10 a fost proiectat să arate *identic* pe computere, laptopuri, tablete și smartphone-uri, utilizând conceptul de *Universal Apps*. Prin *Cross-platform*, posesorii de echipamente cu *iOS* și *Android* pot rula aplicații specifice lui *Windows 10*. Și reciproca este adevărată, *Windows 10* putând să ruleze aplicații specifice sistemelor de operare *iOS* și *Android*.

Configurare

Settings și Control Panel
Control Panel propriu
God Mode
Start Meniu identic pe toate computerele
Controlul nivelului de acces al utilizatorului
Action Center invizibil
Redirectarea traficului de la Edge la Internet Explorer
Registry Editor

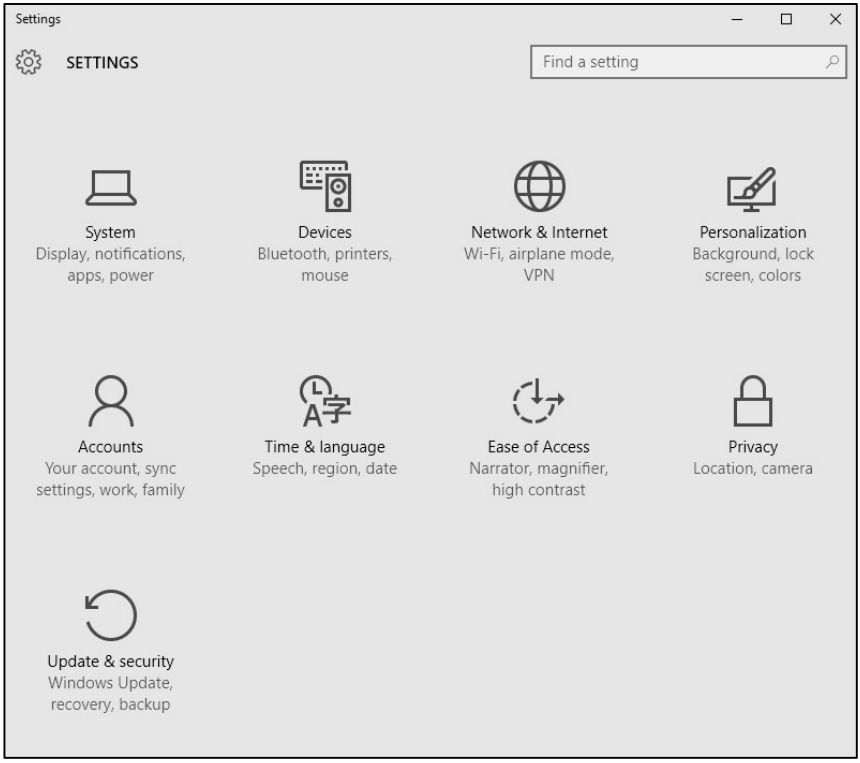
Settings și Control Panel

Vechiul *Control Panel* controlează majoritatea setărilor din Windows 10, fiind rezervat utilizatorilor experimentați. Noul *Settings* (Universal Settings app) oferă un acces mai rapid la setări, adresându-se utilizatorilor de nivel mediu.

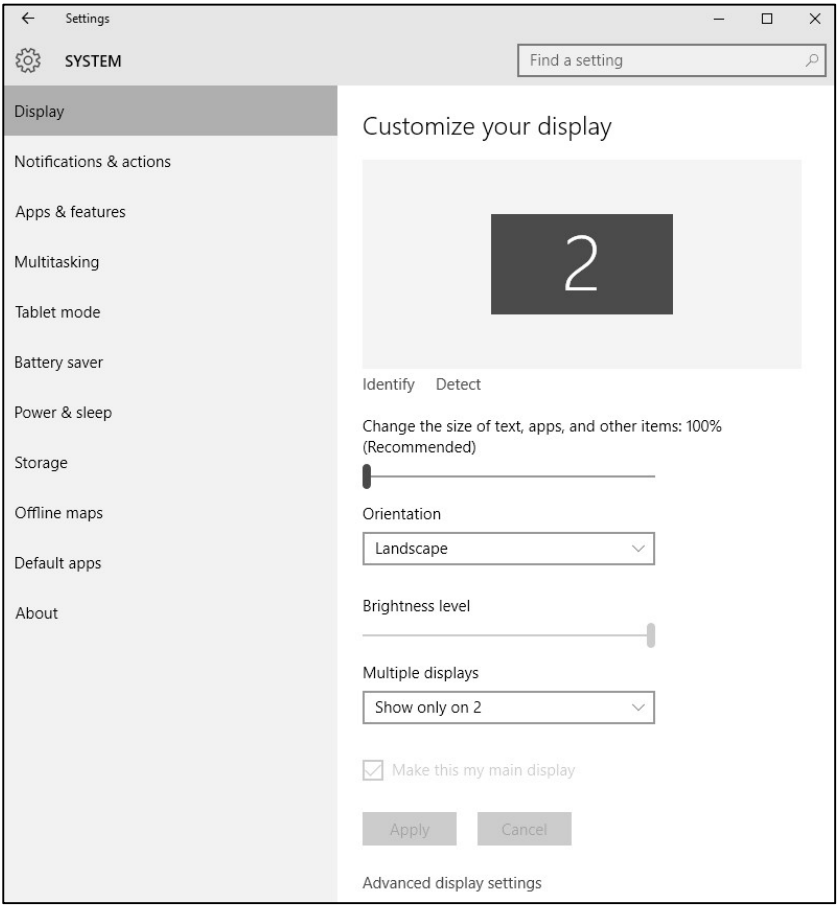
Nici Control Panel şi nici Settings *nu oferă acces complet* la setările din Windows 10, unele setări putând fi efectuate doar din *Control Panel*, iar altele doar din *Settings*.

Settings

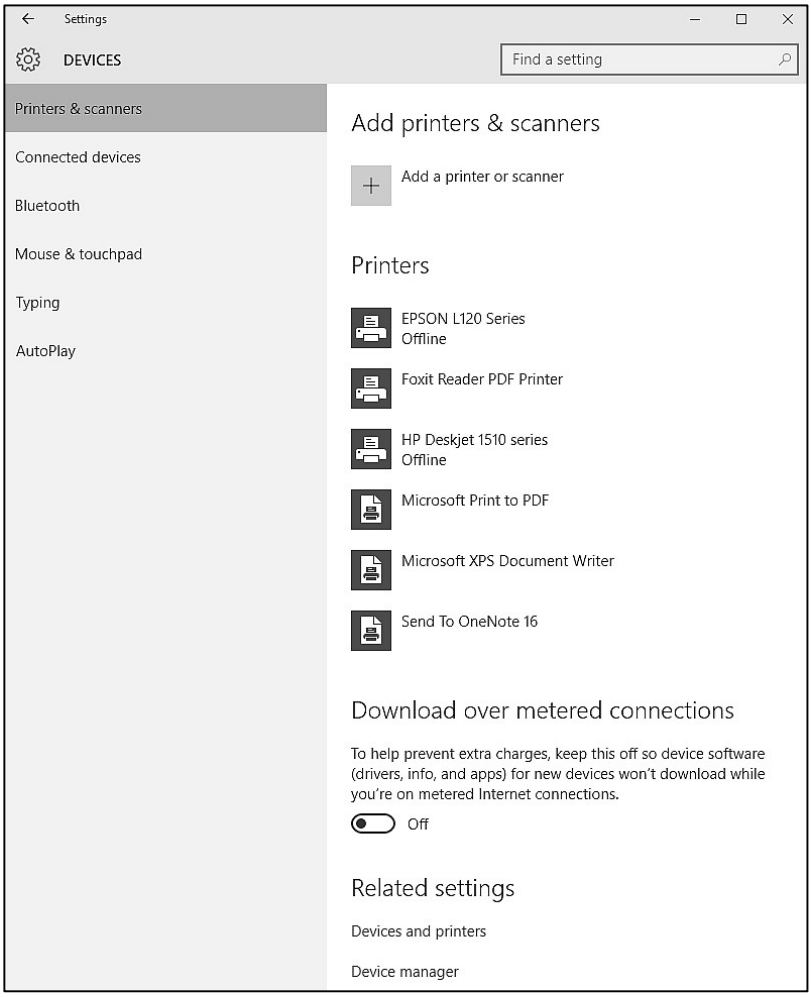
Universal Settings app reprezintă o colecție de setări aranjate într-un mod mai accesibil, dar mai puțin logic decât cele din Control Panel. Pentru a accesa *Settings,* dați clic pe butonul *Start*, apoi alegeți opțiunea *Settings*.



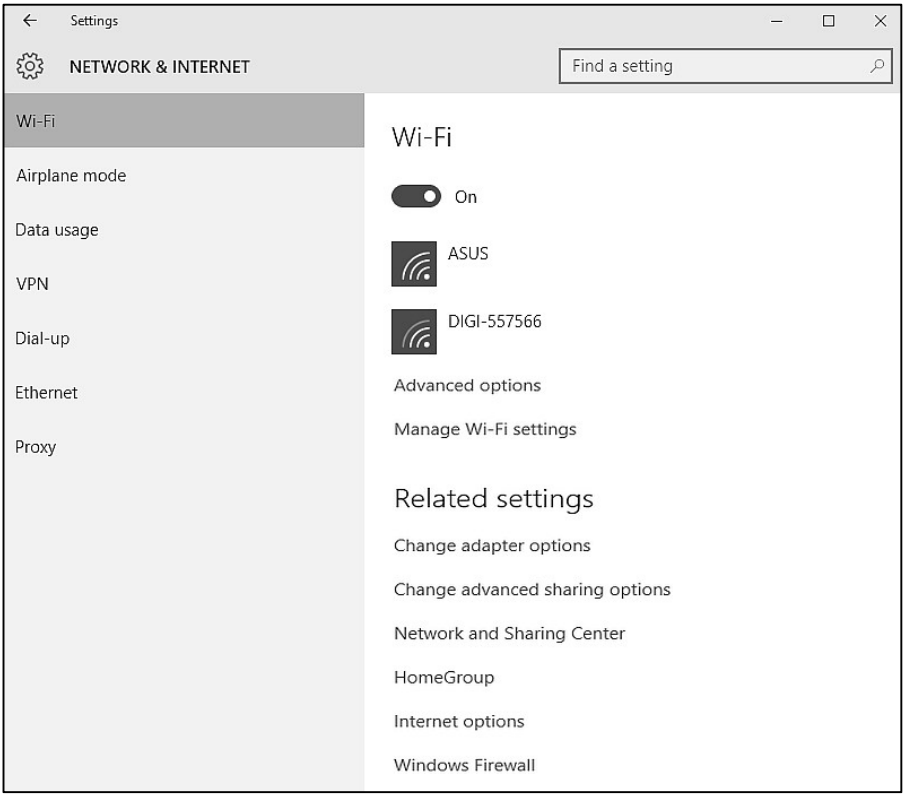
System: Include setări ale display-ului (*Display*) și de control al notificărilor (*Notifications & Actions*), analiza gradului de utilizare a aplicațiilor (*Apps & Features*), manevrarea ferestrelor și desktopurilor virtuale (*Multitasking*), configurarea modului tabletă (*Tablet Mode*), economisirea bateriei (*Battery Saver*), perioadele de pauză (*Power & Sleep)*, analiza spațiului de memorare utilizat (*Storage*), descărcarea și actualizarea hărților (*Offline Maps*), aplicațiile implicite asociate extensiilor (*Default apps*) și numele computerului, domeniul, Azure AD, Device Manager, unelte administrative sau BitLocker (*About*)



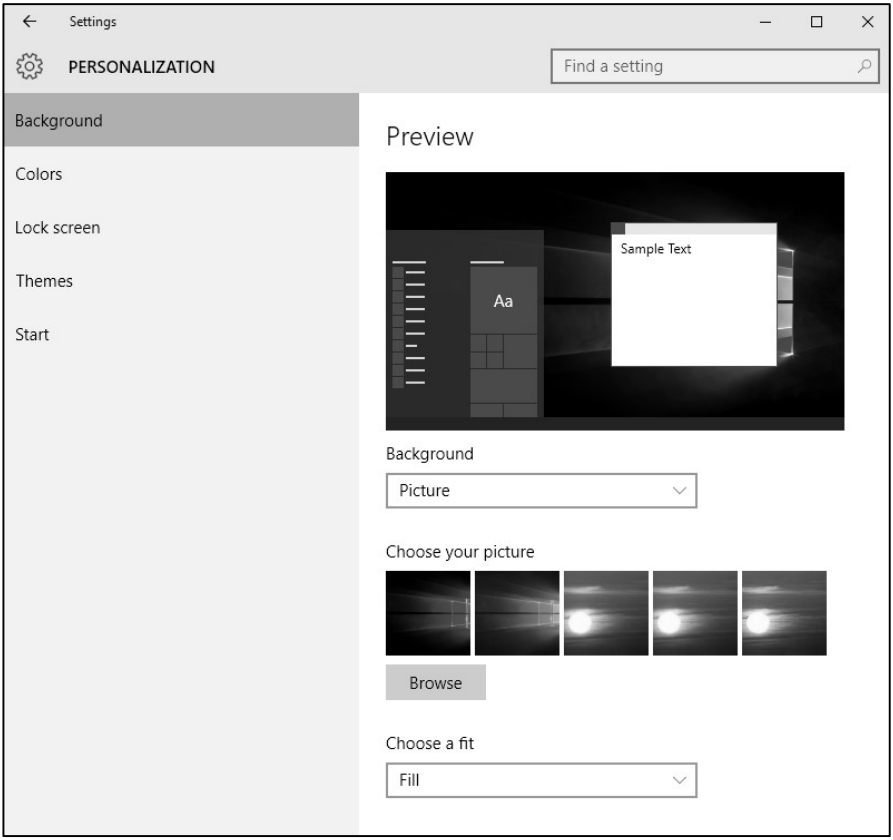
Devices: De aici se pot controla imprimantele, scannerele (*Printers & Scanners*) şi alte dispozitive conectate (*Connected devices*), se poate opri sau porni Bluetooth-ul (*Bluetooth*), se pot seta mouse-ul şi tastatura tactilă (*Mouse & Touchpad*), se poate activa/dezactiva autocorecţia textelor (*Typing*) şi se poate seta modul de redare automată a conţinutului media (*AutoPlay*).



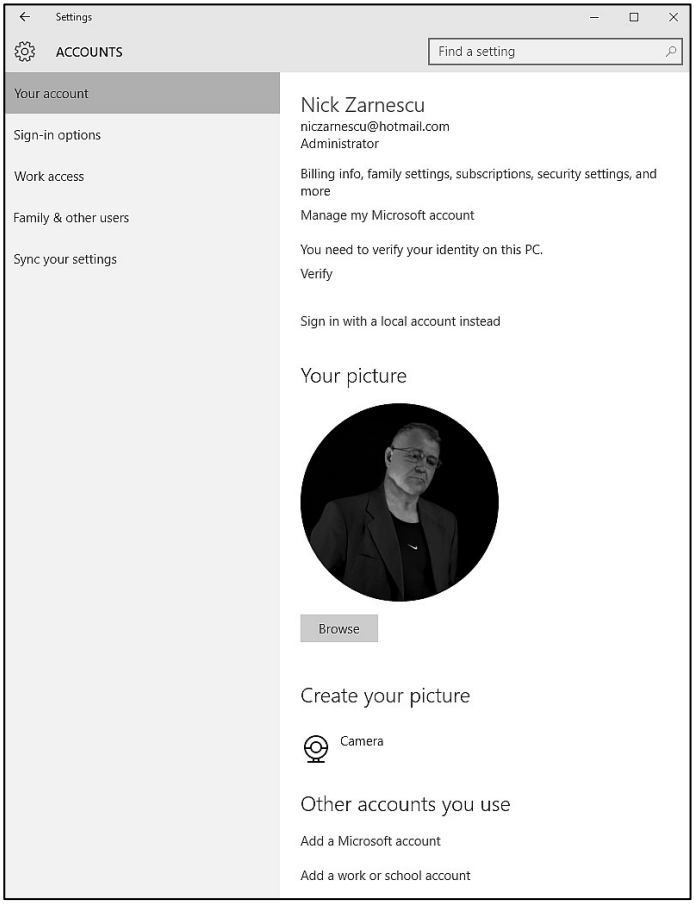
Network & Internet: Permite activarea/dezactivarea Wi-Fi, managementul conexiunilor, legături către Control Panel, Homegroup sau Firewall (*Wi-Fi*), trecerea în modul avion (*Airplane mode*), afișarea utilizării datelor prin Ethernet sau Wi-Fi (*Data Usage*), crearea conexiunilor securizate (*VPN*), conectarea la un ISP (Internet Service Provider), cum sunt RDS sau Clicknet (*Dial-up*), setarea unei rețele LAN sau WAN (*Ethernet*) și setarea manuală/automată a unui server de proximitate (*Proxy*).



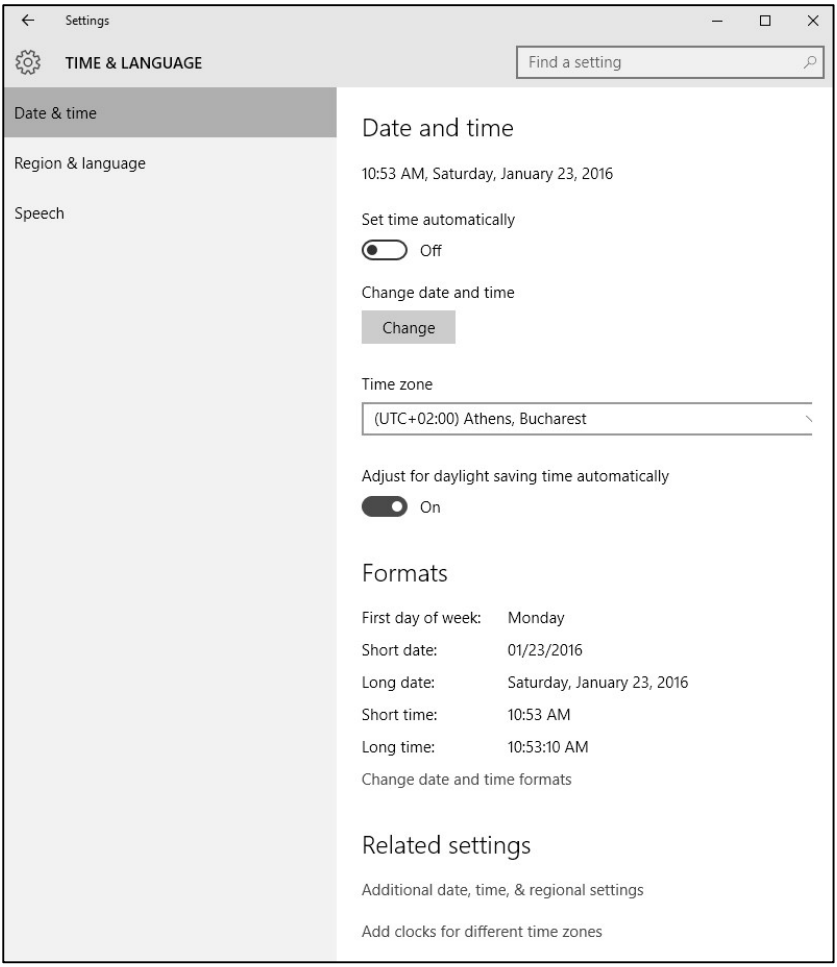
Personalization: Aici puteți schimba imaginea de fundal de pe desktop (*Background*), alege culorile meniurilor (*Colors*), seta imaginea din ecranul de întâmpinare (*Lock Screen*), schimba temele (*Themes*) și controla meniul Start (*Start*).



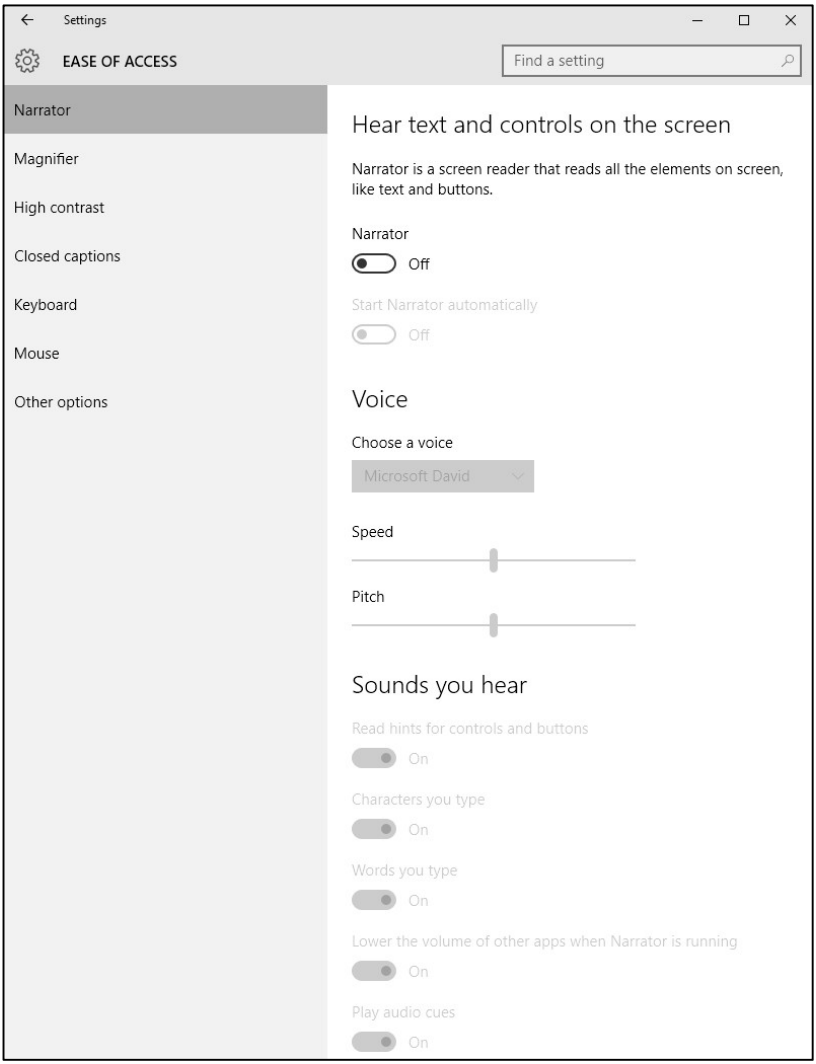
Accounts: Permite deconectarea contului Microsoft şi conectarea cu un cont standard, schimbarea imaginii contului şi adăugarea altor conturi (*Your account*), modificarea parolei, a PIN-ului, a imaginii-parolă şi a facilităţii Hello (*Sign-in options*), conectarea la reţeaua instituţiei, a şcolii sau în cloud, la Microsoft's Azure Active Directory (*Work access*), crearea de conturi pentru membrii familiei (*Family & other users*) şi sincronizarea setărilor între dispozitive (*Sync your settings*).



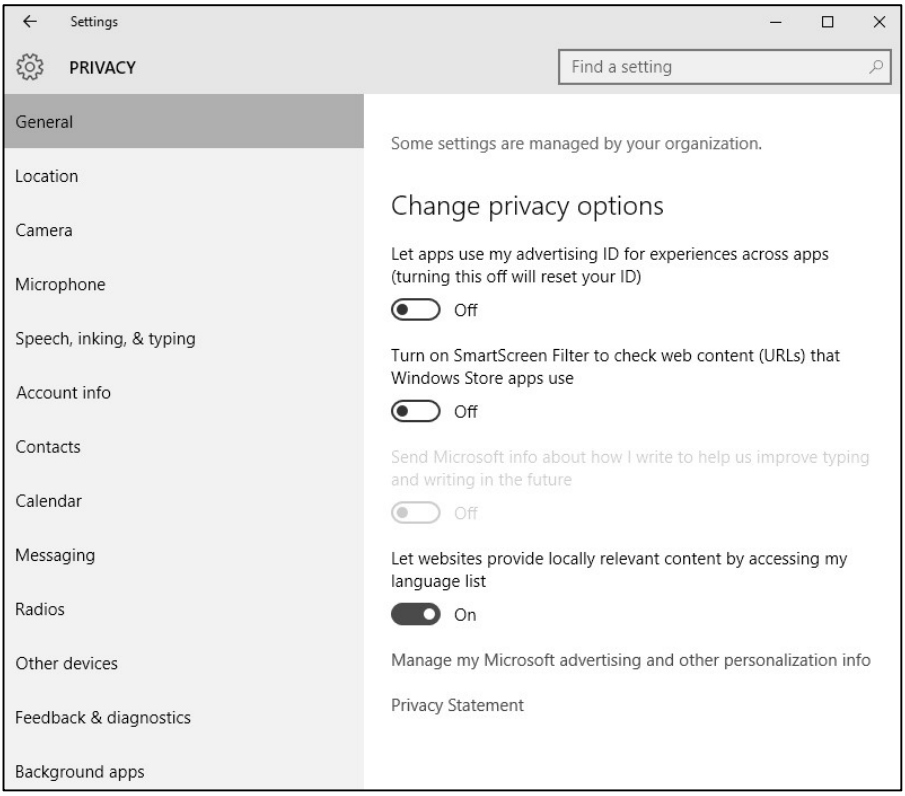
Time & language: Include setări de modificare ale datei și timpului, precum și a formatelor de afișare ale acestora (*Date & Time*), alegerea limbii vorbite, a tastaturii unei anumite țări (*Region & Language*) și calibrarea microfonului pentru recunoașterea optimă a vorbirii (*Speech*).



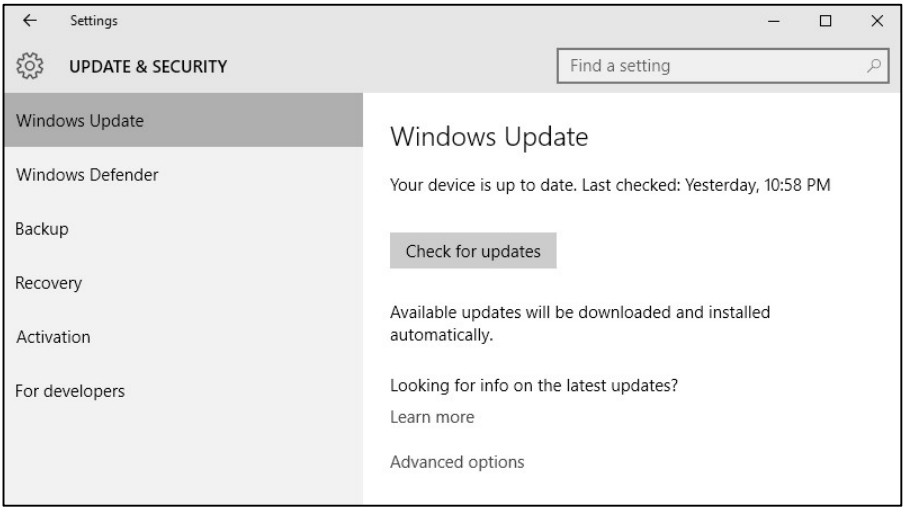
Ease of Access: Această secțiune se adresează mai mult persoanelor cu *dizabilități* și permite configurarea lui Windows 10 în funcție de dificultățile vizuale, auditive sau manuale cu care se confruntă utilizatorii.



Privacy: Microsoft colecționează o mulțime de informații despre utilizatorul computerului, pe care le întrebuințează în scopuri comerciale sau în alte scopuri, atentând la intimitatea persoanei. Modul de utilizare al acestui panou este descris în detaliu în paragraful „*Păstrarea intimității față de Microsoft*“ din volumul „*Windows 10 Ghid practic*”.



Update & Security: Permite efectuarea actualizărilor sistemului de operare (*Windows Update*), configurarea aplicației antimalware (*Windows Defender*), efectuarea operațiunilor de salvare și restaurare (*Backup*), recuperarea datelor prin funcția Reset și prin restartare de pe un stick sau DVD (*Recovery*) sau activarea lui Windows 10 (*Activation*). *Windows 10 Enterprise* are și o secțiune pentru dezvoltatorii de aplicații (*For developers*).

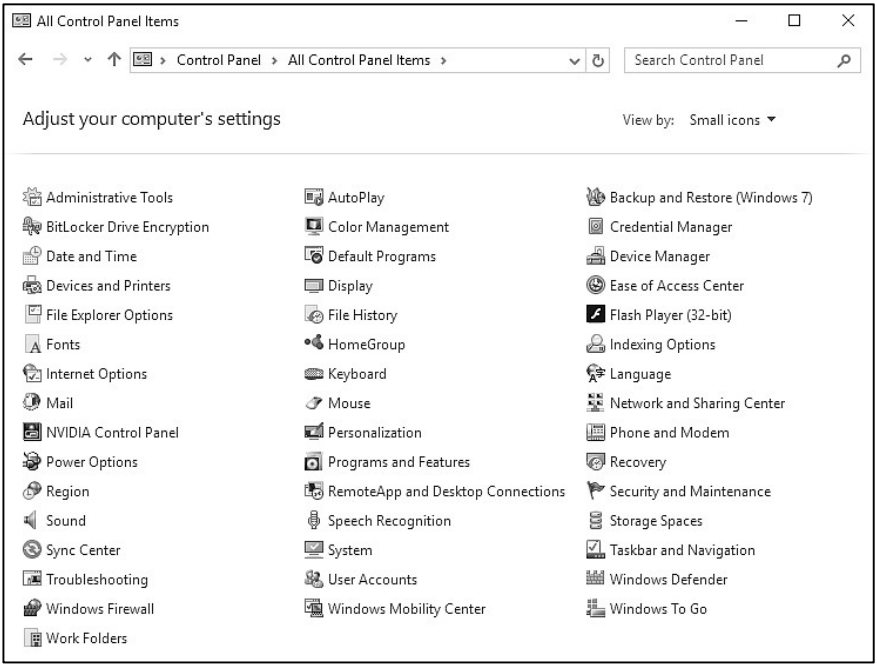


Control Panel

Pentru a lansa Control Panel, se dă clic drept pe butonul *Start* și se alege opțiunea *Control Panel*. Acesta va fi afișat în varianta condensată, cu opt opțiuni (*1. System & Security, 2. Network and Internet, 3. Hardware and Sound, 4. Programs, 5. User Accounts, 6. Personalization, 7. Clock, Language and Region* și *8. Ease of Access*). Pentru a afișa *varianta completă* (vezi pagina următoare), se dă clic pe simbolul „>" aflat în partea din stânga sus a ferestrei, în dreapta lui *Control Panel*, și se alege *All Control Panel Items*. În cele ce urmează vom discuta despre Control Panel în *varianta condensată*.

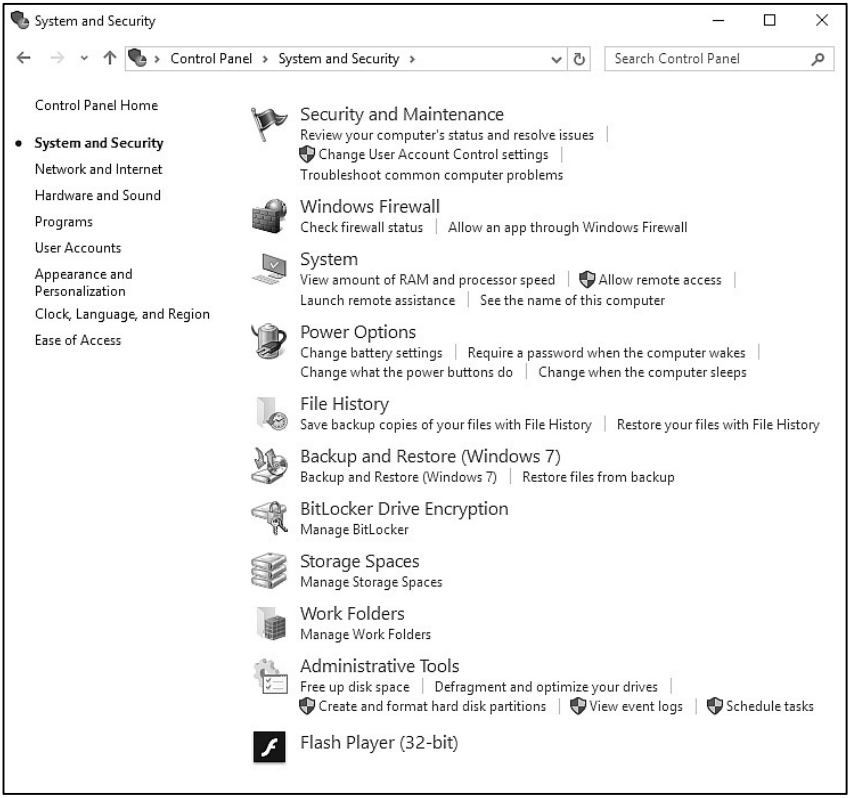


Control Panel – varianta condensată

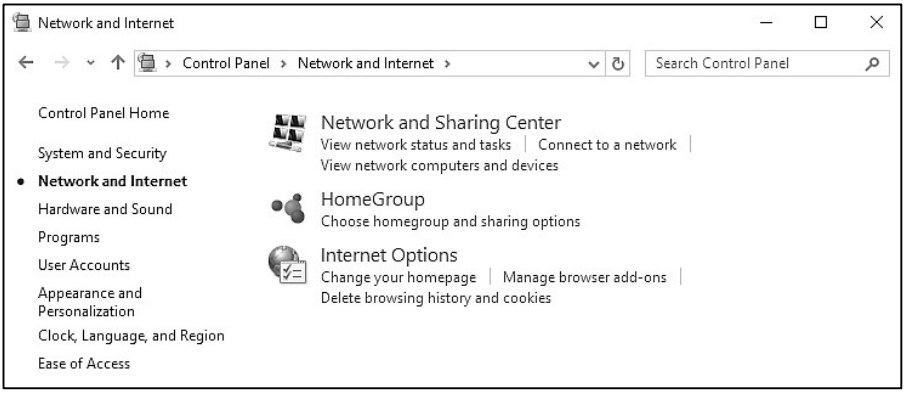


Control Panel – varianta completă

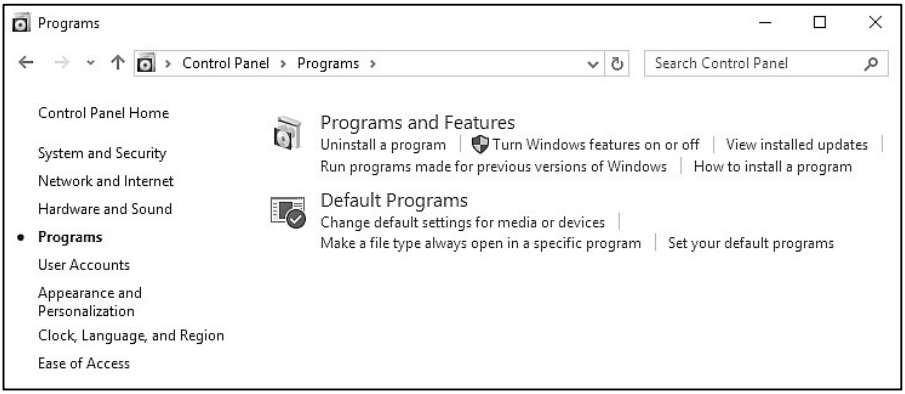
System and Security: Această secțiune este concepută pentru utilizatorii profesioniști. Asigură securitatea și mentenanța sistemului (*Security and Maintenance*), setează Firewall-ul pentru rețele private sau publice (*Windows Firewall*), afișează informații despre performanțele sistemului și despre activarea sistemului de operare (*System*), configurează bateriile laptopurilor pentru un consum minim (*Power Options*), salvează și restaurează fișiere selectate de utilizator (*File History*), salvează și restaurează fișierele sistem și fișierele personale (*Backup and Restore*), activează/dezactivează BitLocker (*BitLocker Drive Encryption*), asigură salvarea datelor pe două sau mai multe drive-uri (*Storage Spaces*), permite utilizarea offline a fișierelor pe mai multe dispozitive (*Work Folders*), oferă unelte de administrare avansate (*Administrative Tools*) și setează Flash Player (*Flash Player*).



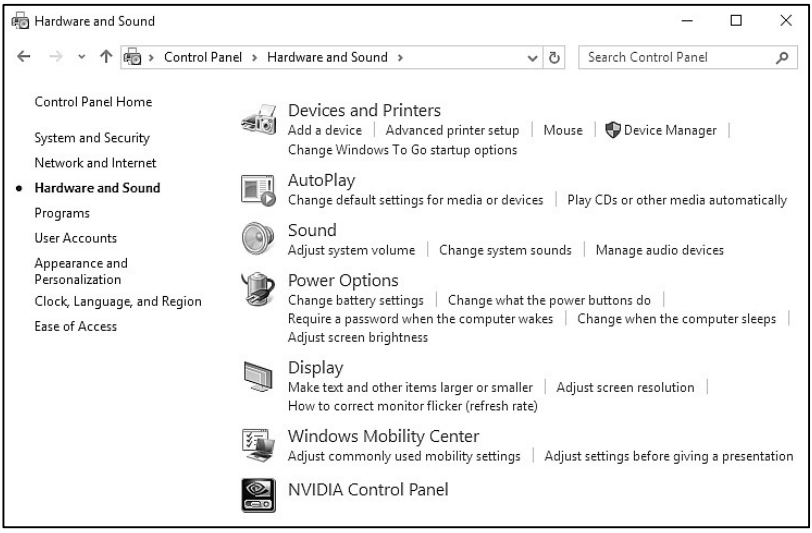
Network and Internet: Permite crearea de noi conexiuni şi setarea acestora în diverse tipuri de reţele (*Network and Sharing Center*), creează HomeGroup-uri pentru partajarea fişierelor în reţea (*HomeGroup*) şi oferă setări avansate de securitate pentru conexiunile la Internet (*Internet Options*).

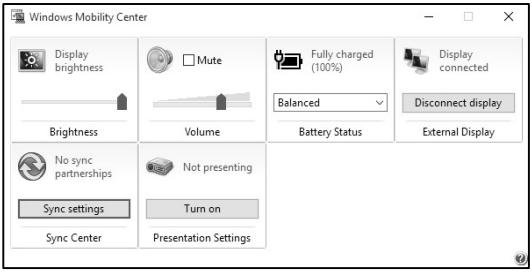


Programs: Permite instalarea aplicaţiilor şi adăugarea de noi facilităţi, precum şi dezinstalarea acestora (*Programs and Features*), asocierea extensiilor de fişiere cu aplicaţii implicite sau aplicaţiile implicite pentru anumite activităţi (*Default Programs*).

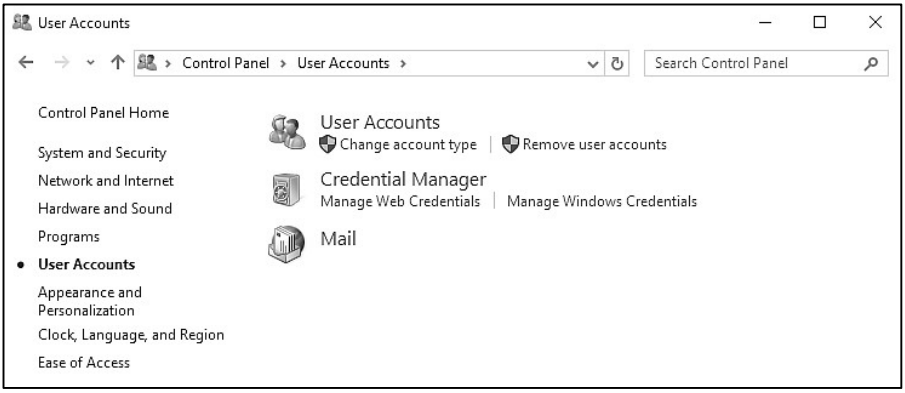


Hardware and Sound: De aici se pot controla imprimantele, scannerele şi alte dispozitive conectate (*Devices & Printers*), se poate seta modul de redare automată a conţinutului media (*AutoPlay*), se pot calibra dispozitivele audio de redare-înregistrare (*Sound*), se poate stabili un plan de încărcare a bateriei laptopului pentru consum minim (*Power Options*), se pot efectua setări avansate ale display-ului şi de afişare pe al doilea display (*Display*), se pot stabili luminozitatea display-ului, nivelul sunetului la redare, afişarea pe două display-uri, sincronizarea informaţiilor şi activarea/dezactivarea unui videoproiector (*Windows Mobility Center*). În cazul nostru apare şi *NVIDIA Control Panel*, prin care se pot efectua setări avansate asupra plăcii grafice şi a display-urilor.

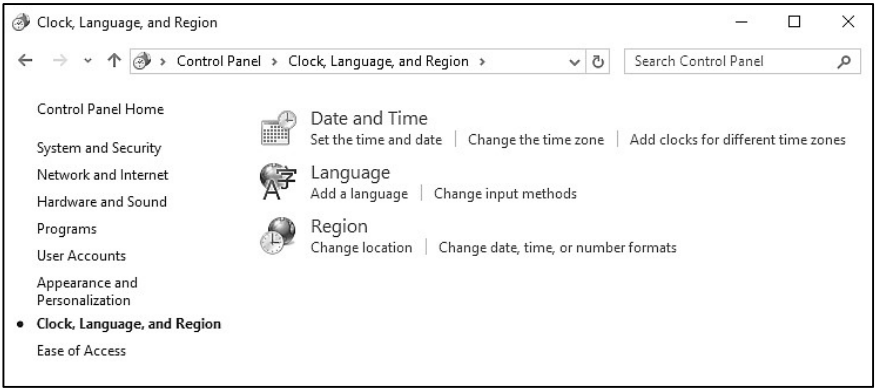




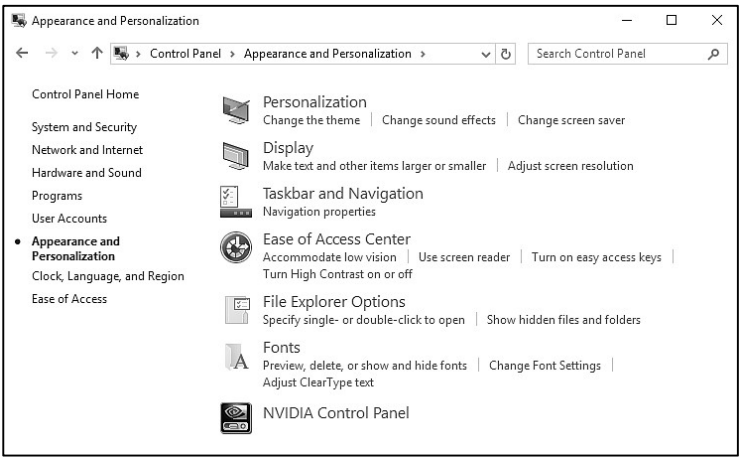
User Accounts: Acest grup cuprinde o selecție limitată de acțiuni pe care Microsoft nu le-a mutat deocamdată în *Settings*. Aici se poate modifica tipul contului, se poate șterge un cont (*User Accounts*), se pot administra credențialele asociate unui cont (*Credential Manager*) sau se pot stabili profiluri de mail pentru Microsoft Outlook (*Mail*).



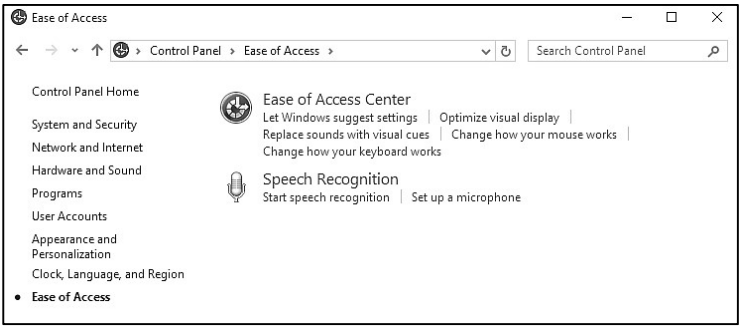
Clock, Language, and Region: Permite setarea datei și a timpului (*Date and Time*), adăugarea de noi limbaje și a tastaturilor asociate (*Language*) și administrarea caracteristicilor unei anumite regiuni geografice: dată, timp, monedă națională și caractere numerice (*Region*).



Personalization: Aici se pot stabili tema vizuală, efectele sonore și setările screen saver-ului (*Personalization*), se pot seta rezoluția display-ului și afișarea pe două display-uri (*Display*), se pot stabili caracteristicile taskbar-ului (*Taskbar & Navigation*), se pot efectua setări pentru persoanele cu dizabilități (*Easy of Access Center*), se pot efectua setări avansate ale lui File Explorer (*File Explorer Options*) sau se pot previzualiza fonturile și se pot efectua modificări asupa caracteristicilor acestora (*Fonts*).



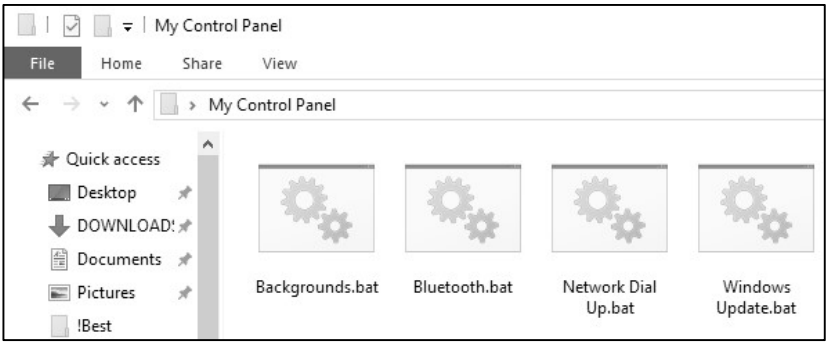
Ease of Access: Permite efectuarea setărilor pentru persoane cu dizabilități (*Ease of Access Center*) și setarea microfonului pentru recunoașterea optimă a vorbirii (*Speech Recognition*).



Control Panel propriu

Windows 10 oferă acces la opțiuni din *Settings* cu comenzi ce pot fi executate prin intermediul *batch*-urilor (.bat). Pentru a vă crea *propriul Control Panel*, creați pe desktop un folder pe care-l puteți denumi *My Control Panel*. În acest folder veți pune *batch*-urile către panourile din *Settings*.

Creați cu Notpad batch-ul *Acount Info.bat*, în care introduceți comanda *start ms-settings:privacy-accountinfo*. Se procedează identic pentre celelale batch-uri pe care le veți utiliza mai des. Astfel vă veți configura *propriul Control Panel*.



Shortcut-uri către Settings

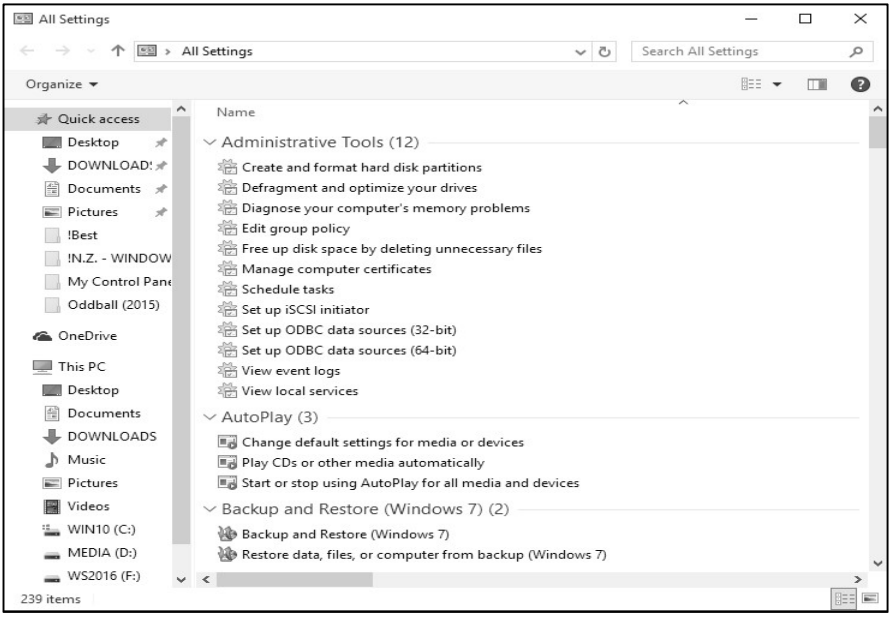
Aplicația din Settings	*Comanda*
Account Info	ms-settings:privacy-accountinfo
Airplane Mode	ms-settings:network-airplanemode
Backgrounds	ms-settings:personalization-background
Battery Saver	ms-settings:batterysaver
Battery Saver Settings	ms-settings:batterysaver-settings
Battery Use	ms-settings:batterysaver-usagedetails
Bluetooth	ms-settings:bluetooth
Calendar	ms-settings:privacy-calendar
Camera	ms-settings:privacy-webcam
Cellular	ms-settings:network-cellular
Closed Captioning	ms-settings:easeofaccess-closedcaptioning
Colors	ms-settings:colors
Colors	ms-settings:personalization-colors
Connected Devices	ms-settings:connecteddevices
Contacts	ms-settings:privacy-contacts

Data Usage	ms-settings:datausage
Date and Time	ms-settings:dateandtime
Dial-up	ms-settings:network-dialup
DirectAccess	ms-settings:network-directaccess
Display	ms-settings:display
Display	ms-settings:screenrotation
Ethernet	ms-settings:network-ethernet
Family Other Users	ms-settings:otherusers
Feedback	ms-settings:privacy-feedback
For Developers	ms-settings:developers
High Contrast	ms-settings:easeofaccess-highcontrast
Keyboard	ms-settings:easeofaccess-keyboard
Location	ms-settings:privacy-location
Lockscreen	ms-settings:lockscreen
Magnifier	ms-settings:easeofaccess-magnifier
Manage Wi-Fi Settings	ms-settings:network-wifisettings
Messaging	ms-settings:privacy-messaging
Microphone	ms-settings:privacy-microphone
Mobile Hotspot	ms-settings:network-mobilehotspot
Motion	ms-settings:privacy-motion
Mouse	ms-settings:easeofaccess-mouse
Mouse Touchpad	ms-settings:mousetouchpad
Narrator	ms-settings:easeofaccess-narrator
Notifications Actions	ms-settings:notifications
Offline Maps	ms-settings:maps
Optional Features	ms-settings:optionalfeatures
Other Devices	ms-settings:privacy-customdevices
Other Options (Ease of Access)	ms-settings:easeofaccess-otheroptions
Personalization	ms-settings:personalization
Power Sleep	ms-settings:powersleep
Privacy	ms-settings:privacy
Proximity	ms-settings:proximity
Proxy	ms-settings:network-proxy
Radios	ms-settings:privacy-radios
Region Language	ms-settings:regionlanguage
Sign-in Options	ms-settings:signinoptions
Speech	ms-settings:speech
Speech, Inking, Typing	ms-settings:privacy-speechtyping

Start	ms-settings:personalization-start
Storage Sense	ms-settings:storagesense
Tablet Mode	ms-settings://tabletmode/
Themes	ms-settings:themes
Typing	ms-settings:typing
VPN	ms-settings:network-vpn
Wi-Fi	ms-settings:network-wifi
Windows Update	ms-settings:windowsupdate
Work Access	ms-settings:workplace

God Mode

Windows 10 oferă o colecție de *239 de shortcut-uri* către setări cuprinse în *Settings* sau în *Control Panel*, alcătuind așa numitul *God Mode* (Modul Divin). Pentru a accesa God Mode, se creează pe desktop un folder care va purta denumirea *GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}*. Folderul va avea, în mod automat, *aceeași pictogramă* ca și *Control Panel*. Se poate utiliza și alt nume în loc de GodMode, de exemplu *All Settings*.



Start Menu identic pe toate computerele

Dacă vreți ca *Start Menu* să arate identic pe toate computerele dintr-o rețea, atunci creați pe computerul administratorului folderul *Layouts* în partiția C.

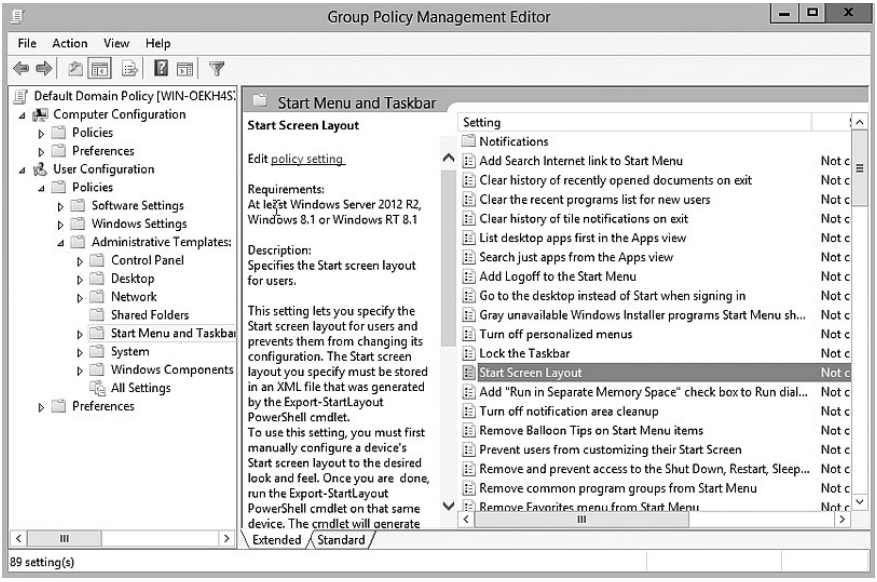
Tastați *PowerShell* în căsuța de căutare pentru Cortana, dați *clic drept* pe *Windows PowerShell (Desktop App)* și selectați *Run As Administrator*.

În *PowerShell* introduceți comenzile următoare:

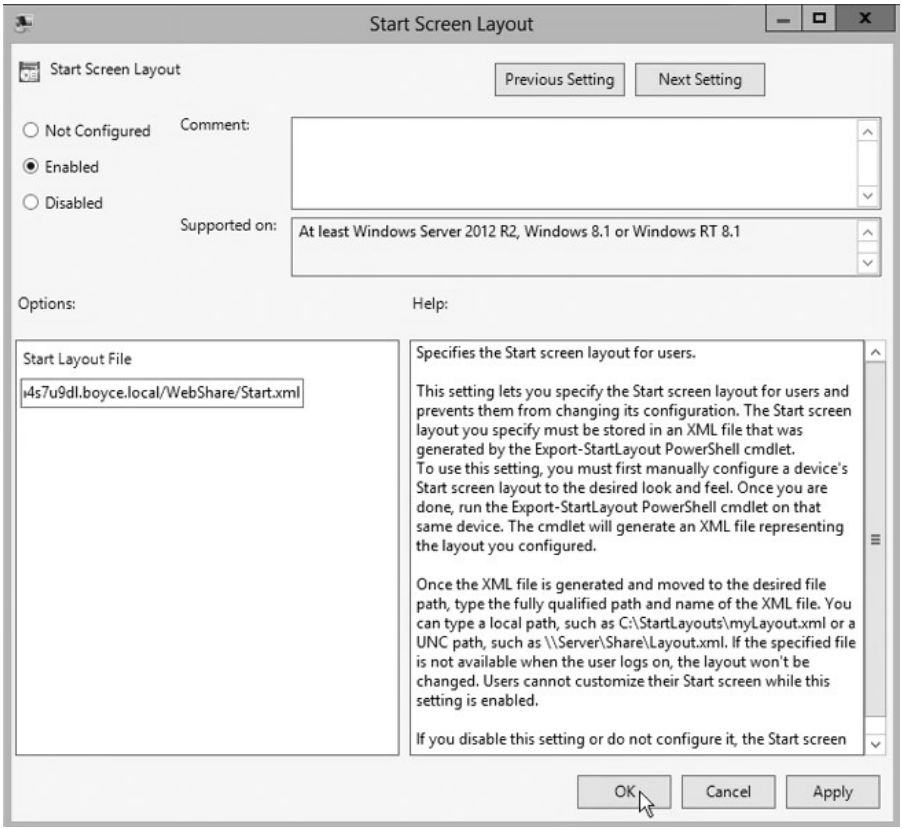
PS C:\Windows\system32>*cd \layouts*

PS C:\layouts>*Export-StartLayout -Path "c:\layouts\start.xml"*

PowerShell va crea în folderul Layouts fișierul *start.xml*, care va putea fi utilizat pentru celelalte computere. Copiați fișierul *start.xml* în folderul *WebShare* din partiția C a serverului cu *Windows Server*, apoi deschideți *Group Policy Management Editor*. Expandați arborele următor: *Default Domain Policy – User Configurations – Policies – Administrative Templates – Start Menu and Taskbar*, unde veți găsi opțiunea *Start Screen Layout*.



Dați dublu clic pe *Start Screen Layout*, iar în fereastra care apare dați clic pe *Enable*, după care introduceți calea completă a fișierului *start.xml* în căsuța *Start Layout File* și apăsați butonul *OK*.



Din acest moment, *Start Menu* va arăta *identic* pe toate computerele și *nu va mai putea fi modificat de utilizatori*.

Controlul nivelului de acces al utilizatorului

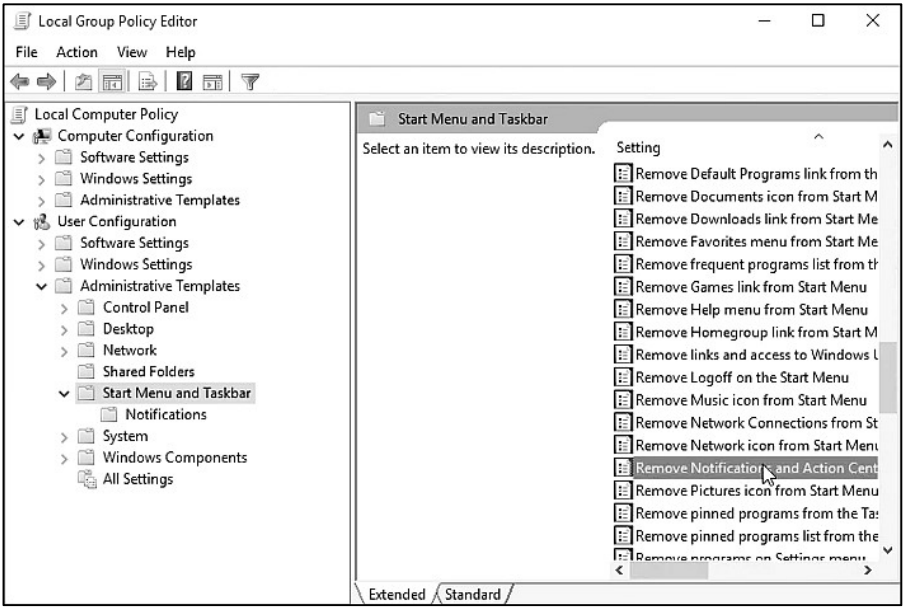
Pentru a stabili nivelul de acces al unui utilizator la aplicațiile care vor fi rulate sau instalate, se urmează calea *Start – Control Panel – User Accounts – User Accounts – Change User Account Control settings*. Cele patru nivele sunt cuprinse între *Always Notify* (notificări permanente) și *Never Notify* (accesul la aplicații este total, dar și foarte riscant în același timp). Nivelul 2 constituie cea mai bună alegere, iar nivelul 4 (*Never Notify*) nu este recomandat.

Action Center invizibil

Charms din Windows 8 a fost înlocuit în Windows 10 cu *Action Center*, care poate fi deschis prin *clic* pe butonul din dreapta difuzorului din Taskbar. În partea superioară apar notificările despre starea dispozitivelor, iar în partea inferioară există tile-uri pentru setările acestora.

Dacă apăsați tile-ul *All Settings* și deschideți panoul *System*, selectând *Notifications & Actions*, puteți face setări ale modului în care poate să se comporte *Action Center*.

Tastați *Local Group Policy Editor* în căsuța de căutare pentru Cortana, alegeți *Local Group Policy Editor*, expandați arborele *Local Computer Policy – User Configuration – Administrative Templates – Start menu and Taskbar* și derulați în dreapta până găsiți opțiunea *Remove Notifications and Action Center*.

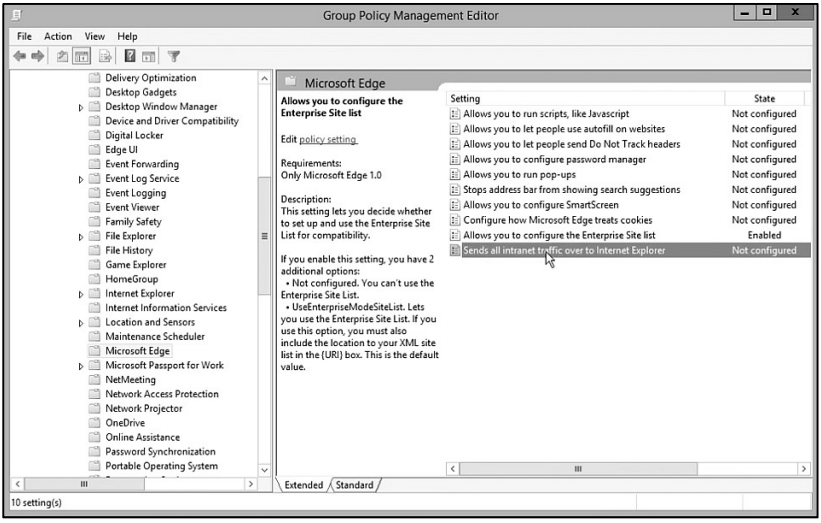


Dați *dublu clic* pe opțiunea respectivă și selectați *Enabled* în fereastra care se deschide, apoi apăsați butonul *OK*. Butonul *Notifications* va dispărea de pe Taskbar, dar utilizatorul va putea vedea în continuare mesajele afișate de acesta, fără a mai putea însă efectua modificări în Action Center.

Redirectarea traficului de la Edge la Internet Explorer

Dacă în rețeaua locală aveți aplicații care funcționează doar cu *Internet Explorer*, puteți redirecta traficul de la *Microsoft Edge* la acesta.

Deschideți *Group Policy Management Editor* pe serverul Windows Server 2012 R2 și expandați arborele *Default Domain Policy – Policies – Administrative Templates – Windows Components – Microsoft Edge*, dați dublu clic pe opțiunea *Sends all intranet traffic over to Internet Explorer*, apoi selectați *Enabled* și apăsați *OK*.



Registry Editor

Prin Registry Editor se poate accesa baza de date a lui Windows 10, care conține sistemul de *regiștri*, informații despre *driverele* utilizate, *parolele* utilizatorilor precum și alte *informații* despre organizarea sistemului de operare.

Registy Editor poate fi accesat în mai multe moduri: 1. Dați clic drept pe *Start*, alegeți *Run* și tastați *regedit* în dreapta lui *Open* din căsuța care apare; 2. În folderul *C:\Windows* lansați *regedit.exe*; 3. Apăsați *Windows+X*, alegeți *Command Prompt*, apoi tastați *regedit*; 4. Tastați *Power* în căsuța de căutare, alegeți *Windows PowerShell*, apoi tastați *regedit*; 5. Creați un shortcut către *C:\Windows\regedit.exe*.

Windows PowerShell este *un Command Prompt* cu posibilități extinse.

Securitate

Securitatea în Windows 10
Securizarea hardware
Securizarea identităților
Securizarea software

Securitatea în Windows 10

Elemente suplimentare de protecţie

Începând din 2002, de la iniţiativa *Trustworthy Computing* (încrederea în computer), fiecare versiune nouă de Windows a introdus elemente semnificative în ceeea ce privește securitatea computerelor din instituţii, cele mai cunoscute fiind *Windows Defender* şi *SmartScreen filter*, care blochează ameninţările venite din exteriorul reţelei.

Windows 10 asigură şi o *protecţie hardware*, care intră în acţiune înainte de bootarea sistemului de operare. De asemenea, este prezentă şi o *securitate bazată pe un server de încredere din reţea*, căruia administratorul reţelei îi aplică o *politică de grup* (Group Policy) corespunzătoare.

Identitatea utilizatorului poate fi ascunsă prin proceduri sofisticate, precum *renunoaşterea amprentei, recunoaşterea facială* sau *scanarea irisului*. Parola poate fi acum şi de tip *imagine*, asupra căreia se execută *trei mişcări rectilinii* sau *circulare*. De asemenea, logarea se poate face şi tastând un *cod PIN*.

Tipuri de ameninţări

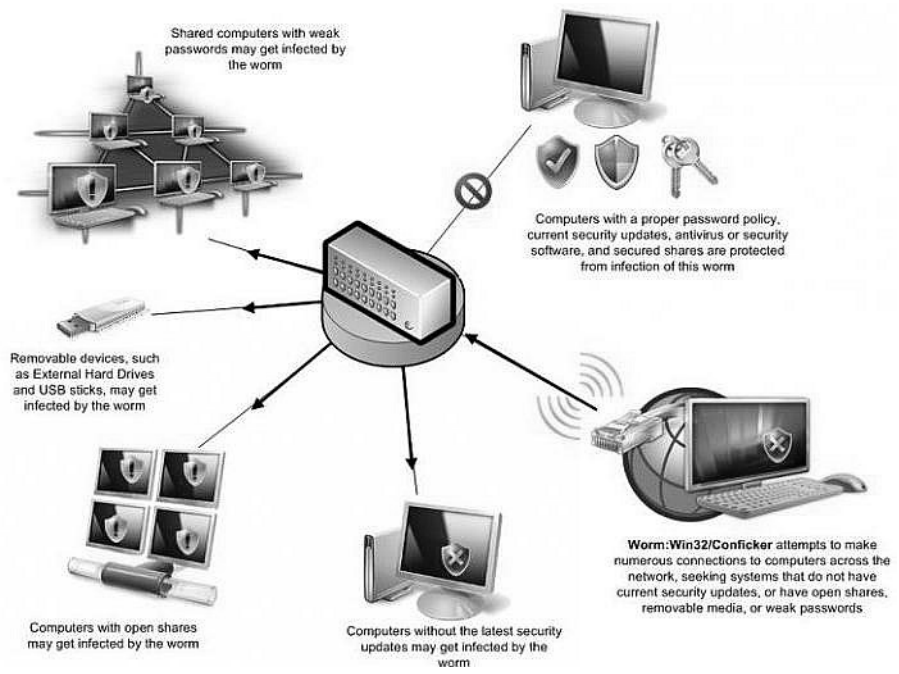
În prezent există grupări criminale care provoacă atacuri cibernetice asupra marilor organizaţii, furând identităţile angajaţilor şi provocând pagube importante.

Atacurile *malware* (inserarea de coduri distructive în aplicaţii) şi *phishing* (furtul informaţiilor bancare prin email-uri false, vezi *www.millersmiles.co.uk*) sunt cele mai întâlnite. Mai există şi *atacuri ţintă* (targeted attacs) al căror scop este de a exploata breşele de securitate ale marilor organizaţii (*ZeroDay Exploits*).

Cele mai multe atacuri se desfăşoară prin *social engineering* (exploatarea reţelelor de socializare), unde atacatorii pretind a fi angajaţi ai unei instituţii foarte cunoscute, solicitând *datele personale* ale celui care accesează reţeaua de socializare (adresa de email, codul numeric personal, PIN-ul cardului etc.).

Alte atacuri se produc prin afişarea unor mesaje care avertizează utilizatorul că *nu are instalată o versiune corespunzătoare a unei aplicaţii* (Java, Flash Player, Adobe Reader etc.) sau că *are computerul infectat* şi i se recomandă descărcarea unei aplicaţii care să înlăture viruşii respectivi. În ambele cazuri, printr-un simplu clic de acceptare (*Backdoor*), computerul va fi atacat, dacă nu există o aplicaţie antivirus foarte performantă. *Zeus*, *Rustock*, *Waledac*, *TDL4/Alureon*, *Conficker*, *Mebroot*, *Mydoom* sau *Sobig* sunt astfel de *backdoor*-uri, care se datorează faptului că utilizatorul nu a efectuat *update-urile reale* ale aplicaţiilor.

În imaginea următoare, publicată de Microsoft, este explicat modul în care acționează virusul *Conficker*.



Prin atacurile *buffer overflow / buffer overrun* (umplerea buffer-ului), atacatorul trimite succesiv date către un anumit buffer, până la umplerea acestuia, blocând funcționarea sistemului de operare.

O rețea de calculatoare poate strangulată (*botnet*) prin rularea unui *keylogger* (un program care trimite în mod *aleatoriu* date către toate computerele, până când acestea încep să funcționeze necorespunzător sau chiar se blochează).

Site-urile rivale pot fi blocate prin atacurile *DoS* (Denial of Service – interzicerea accesului). Atacatorii ghidează mii de utilizatorii de Internet către aceste site-uri, făcându-le astfel *nefuncționale*. Un astfel de atac a fost *Stuxnet*, care a avut ca obiectiv blocarea site-ului official al firmei Siemens. Se vehiculează chiar idea că atacul a fost premeditat de *serviciile secrete* ale anumitor țări.

Există trei site-uri principale care vă pot informa despre cele mai recente tipuri de atacuri informatice:

- Microsoft Security Response Center (MRSC – *blogs.technet.com/b/msrc*);
- Windows Secrets Newsletter (WSN – *www.windowssecrets.com*);
- SANS Internet Storm Center (ISC – *isc.sans.edu*)



În final, vă aducem la cunoștință că fiecare clic pe care-l dați când navigați pe Internet este monitorizat prin *cookie*-uri de ***Doubleclick.net***, care aparține de Google. După ce veți vizita un site, pentru a efectua anumite cumpărături sau pentru a căuta informații importante, la următoarea deschidere a browser-ului veți observa mici reclame care au legătură cu site-urile vizitate anterior.

Dacă utilizați ***Firefox***, atunci urmați calea *Tools – Options – Privacy – Show Cookies* și observați partea inferioară a listei afișate.

Pentru a vedea exact ce cookie-uri vă urmăresc activitatea, instalați ***The Ghostery browser*** (*www.ghostery.com/download*).

Lista tuturor *adreselor de email compromise de hackeri* se află pe site-ul ***PwnedList*** (*www.pwnedlist.com*)

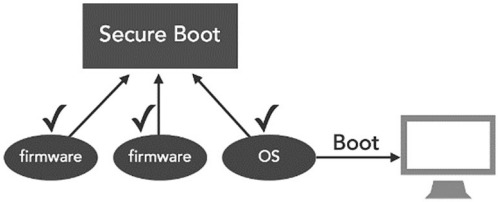
Securizarea hardware

Acest tip de securitate a fost introdus începând cu Windows 8.1. Deşi puteţi instala Windows 10 şi pe computere mai vechi, protecţia noilor tipuri de computere va fi mult mai puternică dacă dispun de următoarele facilităţi:

• ***Unified Extensible Firmware Interface*** *(UEFI – Interfaţa firmware extensibilă unificată)* Arhicunoscutul *BIOS* din PC-uri a fost înlocuit, după 30 de ani, cu UEFI, o interfaţă firmware hardware, care *nu poate fi atacată din exterior* şi care asigură o *bootare sigură* (Secure Boot). Microsoft le-a impus producătorilor originali de echipamente (OEMs – Original Equipment Manufacturers) să asigure această facilitate pe toate computerele care vor fi produse după lansarea lui Windows 8.1, prin programul *Windows Hardware Certification* (cunoscut anterior ca *Windows Logo*).

• ***Trusted Platform Module*** (*TPM – Modul platformă de încredere*) TPM este un cip, uneori inclus în placa de reţea, care suportă un *grad extins de criptare* şi *previne descoperirea certificatelor şi a cheilor de criptare*. TPM execută operaţiuni criptografice, memorează chei pentru volumele cu *BitLocker* şi pentru *cardurile inteligente virtuale* (virtual smartcards) şi *semnează* datele în mod digital, printr-o *cheie privată*, care nu poate fi accesată prin software. De prezenţa TPM-ului depind facilităţi esenţiale de protecţie cum ar fi *BitLocker Drive Encryption*, *Measured Boot* şi *Device Guard*. Cea mai agresivă formă de malware este inserarea atacatorului în procesul de boot (*rootkit* sau *bootkit*), pentru a prelua controlul sistemului de operare înainte ca software-ul antimalware să fie activat. Prin includerea MTP-ului, acest tip de atac este *stopat*.

• ***Secure Boot*** *(Boot securizat)* Această protecţie de bază face parte din *arhitectura UEFI*. Pe un PC cu BIOS-ul clasic, orice persoană poate prelua controlul procesului de bootare utilizând un *încărcător alternativ* al sistemului de operare (alternative OS loader), având apoi accces deplin la resursele sistemului. Dacă *Secure Booot* este *activat*, atunci bootarea se poate face doar utilizând un *OS loader* (încărcător al sistemului de operare) care este *semnat* printr-un *certificat* memorat *în firmware-ul UEFI*. Secure Boot poate fi activat doar pe echipamentele care se încadrează în programul *Windows Hardware Certification*.

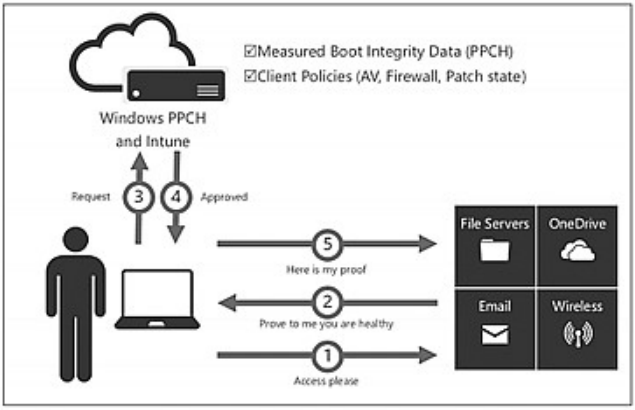


• ***Early Launch Antimalware*** *(ELAM – Lansare preventivă antimalware)* Prin această facilitate, aplicația antimalware *Windows Defender*, semnată și certificată de Microsoft, este lansată *înainte de încărcarea driverelor* oferite de diverși producători ai echipamentelor, permițând astfel detectarea și blocarea încercărilor de intruziune din exterior în timpul procesului de bootare.

• **Trusted Boot** *(Boot de încredere)* Această facilitate verifică *integritatea tuturor componentelor implicate în procesul de bootare*. Încărcătorului (bootloader) i se verifică *semnătura digitală a nucleului* (kernel), înainte de încărcarea acestuia. La rândul său, încărcătorul verifică toate componentele implicate în procesul de bootare (*drivere*, *fișiere de startup* și *ELAM*)

• ***Measured Boot*** *(Boot măsurat)* Cip-ul TPM efectează *măsurători* ale *firmware-ului UEFI* și ale *fiecărei componente implicate în procesul de bootare*. Când aceste măsurători sunt complete, valorile semnate în mod digital și memorate în siguranță în TPM nu pot fi modificate decât la o restartare a sistemului. La bootarea ulterioară, se efectuează același tip de măsurători și se compară cu cele memorate în TPM. Ca măsură suplimentară de securitate, valorile memorate în TPM pot fi semnate și transmise unui *server aflat la distanță* (remote server), care efectuează o comparație suplimentară (*remote attestation*) și atestă siguranța clientului.

• ***Provable PC Health*** *(Integritate demonstrabilă prin PC)* Pentru smartphone-urile dotate cu *Windows 10 Mobile*, Microsoft a introdus o interfață pentru aplicații (*API – Application Program Interface*) care le permite acestor echipamente să acceseze un *serviciu de atestare la distanță* (RAS – Remote Attestation Service) denumit *Provable PC Health (PPCH)*. PPCH poate permite sau interzice accesul la o rețea și la serviciile acesteia, în funcție de rezultatele primite de la RAS.



Procedurile de boot securizat și boot măsurat

Principala problemă de securitate cu care se confruntă sistemele de operare este aceea că *firewallurile* și *antiviruşii* acționează doar *după bootare*. Dacă un hacker reușește să se infiltreze printr-un *rootkit* în procedura de bootare, poate obține controlul asupra sistemului, ascunzându-și software-ul de aplicațiile care ar trebui să protejeze computerul.

Situația devine foarte complicată atunci când angajații utilizează *laptopurile și smartphone-urile personale* (BYOD – Bring Your Own Device), iar acestea sunt conectate la *serverele companiei*. În acest caz ar trebui să existe o *procedură de verificare* a echipamentelor, în timpul bootării acestora, înainte ca aplicațiile de protecție să intre în funcțiune, pentru a fi siguri că sistemele de operare nu sunt infectate.

Windows 8 a introdus procedura *secure boot* (boot securizat), care utilizează firmware-ul *UEFI 2.3.1*, acesta *neputând fi modificat prin software*, stopând accesul hackeriilor la secvența de boot. Toate componentele sunt verificate printr-o *semnătură validă*, iar dacă apar *module nesemnate*, atunci acestea sunt blocate înainte ca Windows să booteze.

Windows 10 introduce un nivel de protecție suplimentar prin procedura *measured boot* (boot măsurat), care constă în utilizarea unui *criptocip*. Modul *TPM 2.0* (Trusted Platform Module), cu criptocip, va deveni *obligatoriu* pe toate echipamentele pe care se instalează Windows 10, începând cu august 2016.

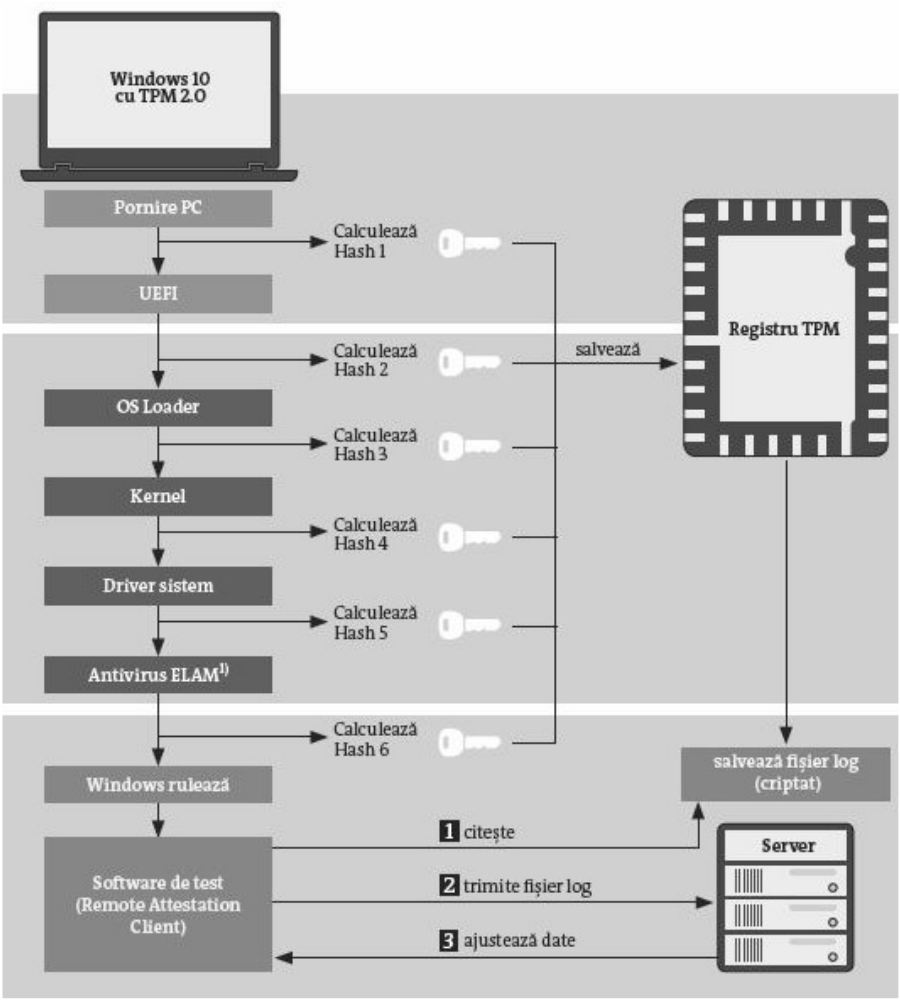
Procedura *measured boot* acționează în felul următor: După pornirea computerului, este calculată o *valoare hash*, asociată cu firmware-ul UEFI, care este salvată într-unul din cei *24 de regiștri de configurare ai TPM* (zone protejate de memorie ce pot fi rescrise doar dacă sistemul rebootează).

Figura din pagina următoare indică modul în care se utilizează procedurile *secure boot* și *measured boot* la încărcarea sistemului de operare.

La început este executat *testul de firmware UEFI*. Loader-ul sistemului, modulele *kernel* și *driverele sistem* calculează *sumele de verificare*, care sunt salvate în *registrul TPM*.

Prin procedura *antivirus ELAM* (Early Lunch AntiMalware) se dă prioritate unui *software de protecție*, precum Kaspersky, Bitdefender sau Symantec, calculându-se o altă *valoare hash*, care este salvată în *TPM*.

Procedura *measured boot* creează un *fișier de log criptat*, care conține o listă a tuturor componentelor încărcate la bootare. Acest fișier poate fi *verificat* ulterior de către un *server de test*, prin funcția *RAS* (*Remote Attestation Service),* avertizând clientul dacă modulele au fost modificate.



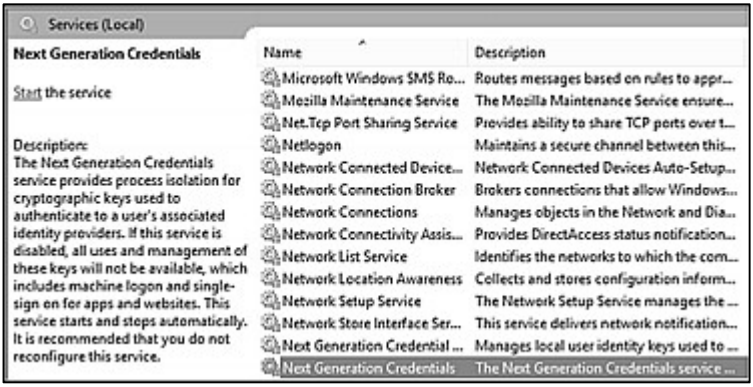
Imagine preluată de pe Internet, apărută și în revista CHIP nr. 9/2015

Securizarea identităților

O tehnică des utilizată de atacatori este furarea *credențialelor* utilizatorilor. De fapt atacatorul nu cunoaște exact numele, parola și alte date, dar are un *stoc de credențiale* pe care le rulează în mod automat, până când obține accesul la computerul respectiv. Această tehnică poartă numele *de Pass the Hash Attack* (atac prin trecere peste credențiale derivate).

Windows 10 include *schimbări fundamentale de arhitectură* destinate să prevină astfel de atacuri. Credențialele utilizatorilor sunt mutate într-un mod de securitate virtual (*Virtual Secure Mode*), care este același *container protejat Hyper-V*, utilizat pentru *serviciile de integritate Windows Code*.

Windows 10 a mai implementat un serviciu denumit *generația de credențiale a viitorului* (Next Generation Credentials), asigurând protecție maximă.



Deși *autentificarea multifactor* (MFA) este disponibilă pentru multe echipamente și servicii de astăzi, aceasta este limitată la soluții precum *cardurile inteligente* (smartcards) sau *aplicații de autentificare* de pe smartphone-uri. Windows 10 își construiește autentificarea multifactor chiar în echipamentul și în sistemul de operare instalat pe acel echipament, eliminând *necesitatea unor periferice adiționale* pentru menținerea securității. Pasul cel mai important făcut de Windows 10 este *înglobarea dispozitivului respectiv chiar în echipamentul utilizatorului* sau *în sistemul de autentificare al unei instituții*.

Astfel, noile echipamente includ suport hardware pentru *autentificarea biometrică* (recunoașterea amprentelor, recunoașterea facială și scanarea irisului – *Windows Hello*). Pentru *recunoașterea amprentelor* sunt necesare mai multe treceri ale degetului respectiv peste dispozitivul de recunoaștere, pentru a elimina orice asemănare cu altă amprentă, iar pentru *recunoașterea facială* sunt utilizate razele infraroșii, pentru a elimina posibilitatea recunoașterii feței după o fotografie. Pentru *scanarea irisului* sunt utilizate camere web de înaltă fidelitate.

Al doilea factor important este introducerea *codului PIN* (similar cardurilor bancare). Dacă echipamentul este furat, accesul la acesta devine imposibil, deoarece chiar dacă se trece de autentificarea biometrică, este obligatorie și introducerea codului PIN.

Dacă echipamentul este dotat și cu *TPM*, chiar dacă cel care a furat echipamentul dintr-o instituție cunoaște *userul* și *parola* persoanei, echipamentul, nemaiflându-se în rețeaua respectivă, *nu se mai poate autentifica* prin TPM la RAS (Remote Attestation Server).

Pentru un atacator devine *imposibil* să fure credențialele unui utilizator utilizând *phishing* sau alte tipuri de *atacuri* asemănătoare. Credențialele sunt generate de însuși Windows 10, printr-o *cheie dublă* (privată și publică) sau prin *certificate de autentificare* generate de structuri PKI (Public Key Infrastructure).

Prin *conturile Microsoft*, *Active Directory* și *Azure Active Directory*, Windows 10 gestionează în mod automat *credențialele criptate* ale utilizatorilor. Serviciile web bazate pe *FIDO (Fast IDentity Online)* și criptosistemele de autentificare *RSA (Rivest + Shamir + Adleman)* vor suporta, de asemenea, acest tip de credențiale.

Pentru *utilizatorii casnici* sunt disponibile doar *Windows Hello* (autentificarea biometrică), *parola tip fotografie* și *codul PIN*.

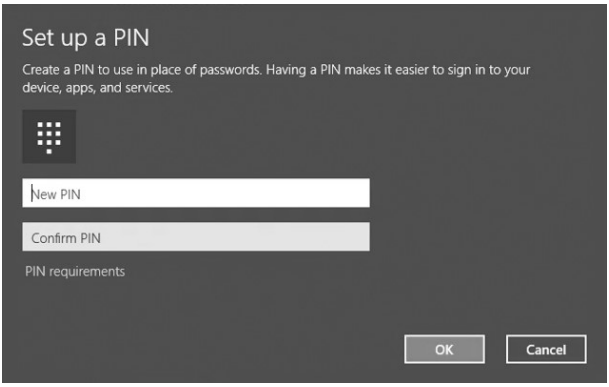


Windows Hello

Pentru a beneficia de facilitățile oferite de *Windows Hello*, urmați calea *Start – Settings – Accounts – Sign-in options* și alegeți un *cod PIN* din minimum 6 caractere numerice. Apăsați butonul *Add* din categoria PIN, apoi introduceți *parola* contului cu care suteți deja logat.



Dacă vreți să știți care sunt cerințele codului PIN, dați clic pe opțiunea *PIN requirements:*



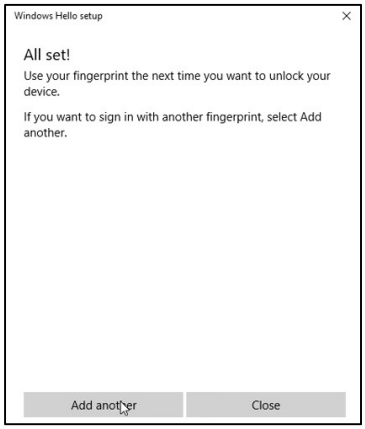
Introduceți codul PIN în căsuța *New PIN*, apoi reintroduceți codul în căsuța *Confirm PIN* și apăsați butonul OK.

Dacă vreți să schimbați ulterior codul PIN, în fereastra *Sign-in options* apăsați butonul *Change* și urmați aceiași pași ca la adăugarea acestuia.

Dacă ați uitat codul PIN, dați clic pe opțiunea *I forgot my PIN* și urmați indicațiile care apar, pentru resetarea PIN-ului.

La următoarea logare, pe ecranul de sign-in va apărea o *căsuță PIN*, în care introduceți codul PIN sau puteți da clic pe opțiunea *Sign-in options*, care vă va permite să alegeți între *logarea cu cod PIN* sau *logarea cu parolă*.



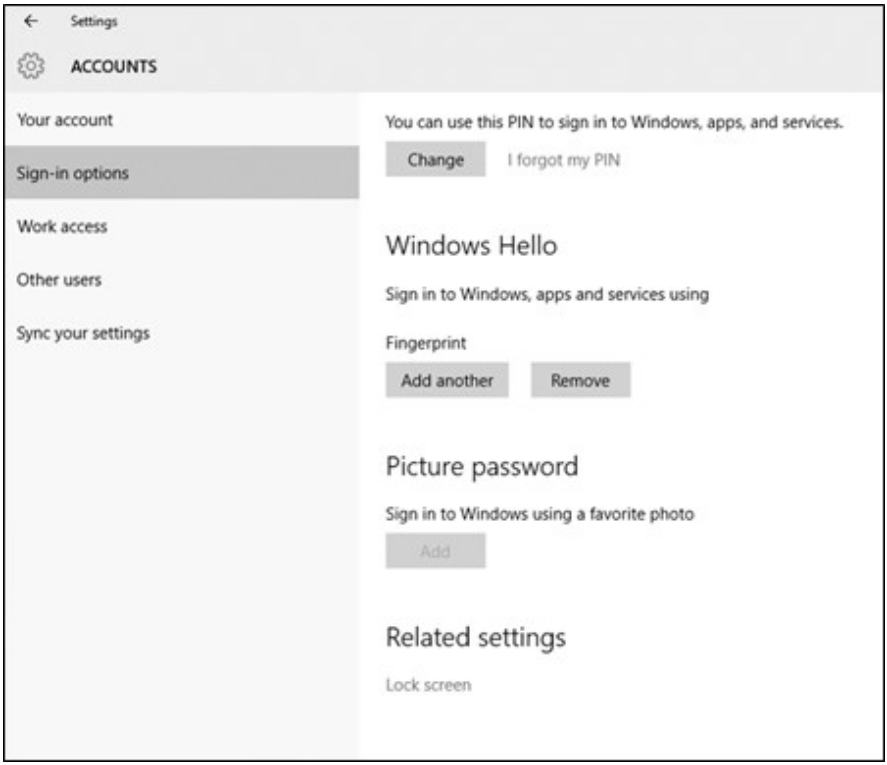


Pentru setarea *logării prin recunoașterea amprentei*, în categoria *Windows Hello* a ferestrei *Sign-in options*, apăsați butonul *Setup* din secțiunea *Fingerprint*, apoi *Get started*, introduceți codul PIN și treceți de câteva ori cu degetul peste dispozitivul de recunoaștere a amprentei.

De îndată ce amprenta a fost recunoscută și memorată, se poate trece la recunoașterea următoarei amprente, dacă vor exista mai multe persoane care vor accesa același echipament.

A doua amprentă poate fi adăugată și ulterior, apăsând butonul *Add another*, sau se poate renunța la recunoașterea amprentei, apăsând butonul *Remove*.

La următoarea încercare de logare va fi suficient să treceți degetul peste dispozitivul de recunoaștere a amprentei și vă veți loga în mod automat.

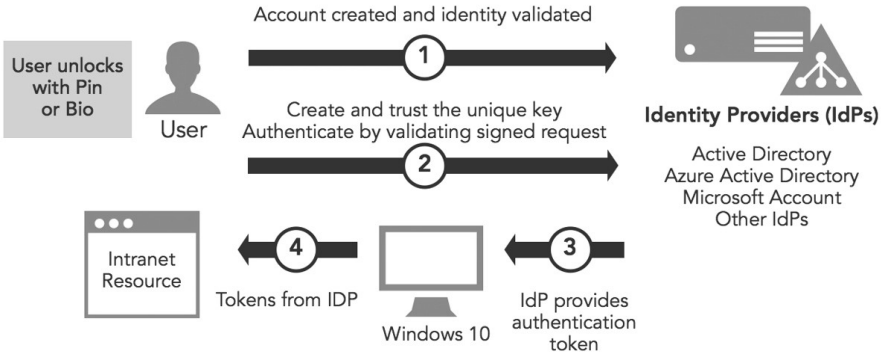


În mod asemănător se procedează și cu *scanarea irisului* sau cu *recunoașterea facială*. Laptopul pe care a fost redactată această carte a permis doar *recunoașterea amprentei*.

Autorul utilizează patru posibilități de logare: *recunoașterea amprentei*, *codul PIN, parola-imagine* și *parola contului Microsoft*.

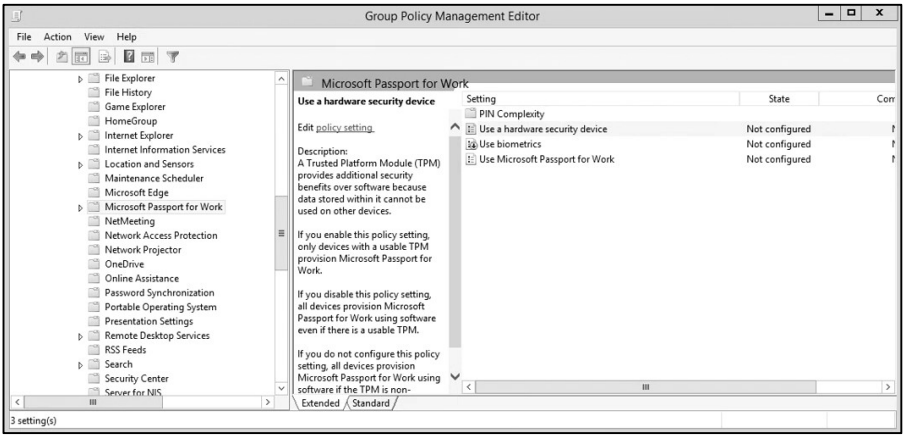
Prin *autentificarea multifactor* (MFA) se introduce o măsură suplimentară de protecție alături de autentificarea biometrică, codul PIN și parole. Astfel, este creat un certificat de autentificare (*Microsoft Passport*), atât printr-o *cheie criptată de TPM*, cât și printr-o *cheie criptată de software*.

Acest mod de autentificare este foarte util atunci când echipamentul este integrat în medii precum *Active Directory* și *Azure Active Directory* sau pentru utilizarea online a *conturilor Microsoft* și a facilității *FIDO* (Fast ID Online).



Imagine preluată din *Microsoft Press – Windows 10 for IT Pros*

Dacă deschideți *Group Policy Management Editor* de pe Windows Server 2012, în arborele din stânga veți găsi ramura *Microsoft Passport for Work:*



În fereastra din dreapta veți putea seta *politicile de utilizare*, atât pentru Microsoft Passport (*Use Microsoft Passport for Work*), cât și pentru autentificarea biometrică (*Use biometrics*), utilizarea TPM-ului (*Use a hardware Security Device*) sau utilizarea codului PIN (*PIN complexity*).

Securizarea software

Blocarea atacurilor din exterior

Windows 10 dispune de două facilităţii de blocare a atacurilor din exterior:

• ***Address Space Layout Randomization (ASLR –*** *Organizarea aleatorie a spaţiului de adrese.***)** Această facilitate organizează în mod aleatoriu datele din memoria computerului, făcând dificilă scrierea în memorie prin atacuri din exterior, deoarece atacatorul nu mai cunoaşte cum sunt organizate datele. Windows 8.1. şi Windows 10 au îmbunătăţit în mod substanţial acest mod de protecţie, în comparaţie cu varianta din Windows 7.

• ***Data Execution Prevention (DEP –*** *Prevenirea executării datelor**)*** Prin această facilitate *se reduce domeniul de memorie* în care codul unei aplicaţii (inclusiv a celei scrise de atacator) poate fi *lansat în execuţie*. Facilitatea DEP a devenit obligatorie începând cu Windows 8.1, iar Windows 10 nu va putea fi instalat dacă această facilitate nu este implementată. DEP utilizează bitul *Never eXecute (NX)* pentru a marca zonele de memorie care stochează date, dar care nu vor putea rula niciodată codul unei aplicaţii

Windows Defender

În Windows 7, *Defender* este o aplicaţie antispyware, cu posibilităţi limitate. Începând cu Windows 8 și continuând cu Windows 10, Defender a devenit o *soluţie de securitate complexă*, capabilă să detecteze toate codurile periculoase care vin din exterior, devenind urmaşul lui *Microsoft Security Essentials*.

Deoarece suportă ELAM, Defender previne *inserarea rootkiturilor* în procesul de boot şi poate *monitoriza comportamentul echipamentelor* dintr-o reţea. Pentru reţelele mari ale instituţiilor, Defender este înlocuit cu *Microsoft's System Center 2012 Endpoint Protection*, care utilizează acelaşi nucleu ca şi Defender şi include ELAM. Desigur, Windows Defender nu oferă un procentaj de securitate de 100%, aşa că pot fi instalate şi aplicaţii antivirus mai performante.

SmartScreen

SmartScreen se bazează pe ideea că este mult *mai eficient* să se *blocheze* un atac din exterior *înainte de executarea codului* atacatorului, decât se îndepărteze codul după inserarea acestuia.

Independent de browserul utilizat, *SmartScreen* verifică orice aplicație în momentul executării acesteia, prin apelarea unei *baze de date Microsoft bazată pe reputație* (Microsoft's application reputation database). Aplicația care nu figurează în baza de date este stopată înainte de executarea acesteia, deoarece se presupune că include *coduri periculoase*, prin care poate fi atacat computerul.

Gradul de protecție cu Smartscreen poate fi stabilit cu *Start – Control Panel – System and Security – Security and Maintenace – Change Windows SmartScreen Settings*. Administratorii pot schimba blocarea automată prin *SmartScreen*, aplicând o politică diferită prin *Group Policy*.

Device Guard

Această nouă facilitate, prezentă doar în *Windows 10 Enterprise Edition*, le permite profesioniștilor IT să blocheze orice aplicație periculoasă care-i tentează pe utilizatori s-o lanseze în execuție, fiind *rulate doar aplicațiile de maximă încredere*.

Chiar dacă atacatorul ar prelua controlul nucleului lui Windows 10, acesta nu-și va putea executa codul său periculos, datorită arhitecturii lui Device Guard, care decide asupra executării aplicației respective, apelând *Windows Code Integrity services* (serviciile de integritate ale codului Windows), care rulează într-un *mod de securitate virtual* (Virtual Secure Mode), un container Hyper-V protejat ce rulează în paralel cu Windows 10. Deciziile de rulare a codurilor aplicațiilor sunt luate pe baza semnăturilor din *firmware-ul UEFI*.

Pentru a putea fi utilizat Device Guard, echipamentele trebuie să aibă anumite *înzestrări speciale*, precum *extensii de virtualizare ale procesoarelor* (Intel VT-x și AMD-V), *SLAT* (Second Level Address Translation), *unități de manangement* (Intel VT-d sau AMD-IOV) și TPM 2.0 (Trusted Platform Module).

În funcție de aceste *înzestrări*, echipamentele se împart în trei categorii: *Device Guard Ready* (toate înzestrările specificate anterior), *Device Guard Capable* (doar o parte din aceste înzestrări) și *Device Guard Not Supported*.

Credential Guard

Tot în Windows Enterprise există *Credential Guard*, prin care se memorează *credențialele* utilizatorilor în anumite spații virtuale protejate (Hyper-V), unde nu pot fi accesate de atacatori. Ca și Device Guard, *Credential Guard* are anumite *cerințe tehnice*: sistem de operare pe 64 de biți, UEFI versiunea 2.3.1 sau mai nouă, Intel VT-x și AMD-V, SLAT, Intel VT-d sau AMD-IOV, TPM 2.0 și Secure Firmware Update.

Windows Defender

Windows Defender vă protejează împotriva virușilor sau aplicațiilor din exterior care pot aduce daune computerului sau pot fura informații prețioase (*malware*).

Setările lui Windows Defender pot fi efectuate urmând calea: *Start – Settings – Update & Security – Windows Defender*.

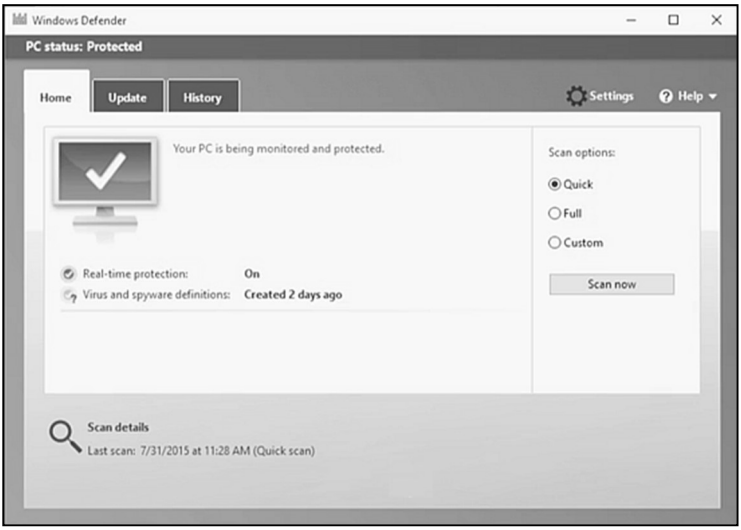


Verificați dacă *Real-time protection* = *On (*Windows Defender este activat). Cu *Cloud-based protection* = *On* și *Sample submission* = *On* ajutați Microsoft să rezolve problemele de securitate, trimițând în cloud informații despre acestea.

Pentru a lansa *Windows Defender*, derulați fereastra *Update & Security* și, în partea inferioară a acesteia, dați clic pe opțiunea *Use Windows Defender*.

În tabul *Home* se pot efectua scanări rapide (*Quick*), complete (*Full*) sau particularizate (*Custom*). Windows Defender efectuează aceste scanări periodic, *în background*, dar, dacă se observă o funcționare anormală a sistemului de operare, pot fi lansate și *în mod expres*.

Dacă instalați un alt antivirus, Windows Defender se va *autodezactiva*, dar el rămâne prezent și poate fi activat oricând, după dezinstalarea antivirusului.



Windows Defender blochează și aplicațiile ce conțin *malware*, pe care încercați să le descărcați de pe anumite *pagini web nesigure*.

Notificările asupra malware-urilor apar în *Action Center* și pot fi șterse prin selectare și clic pe butonul *X*, după ce v-ați asigurat că totul este în regulă.

Windows Defender detectează și *malware*-urile prezente în aplicații de pe *suporturi externe*, atunci când se încearcă lansarea acestora în execuție. Mai mult, izolează aplicația respectivă în *carantină*, de unde poate fi eliminată ulterior.

Este recomandabil să nu accesați pagini web dubioase și să nu deschideți email-uri de la expeditori necunoscuți.

Windows Defender nu asigură o protecție de 100%, așa că puteți instala și alte aplicații cu funcționalitate asemănătoare, cum sunt *Malwarebytes* sau *Spybot Search and Destroy*.

Puteți verifica dacă sistemul de operare are probleme de securitate, apelând funcția *Review*: clic drept pe *Start* – *Control Panel* – clic pe *Review your computer's status*, care se găsește imediat sub categoria *System and Security*. În fereastra care apare, extindeți *Security* și *Maintenance* și veți vedea problemele grave afișate cu culoare *roșie*, precum și modalitățile de rezolvare ale acestora. Problemele potențiale sunt afișate cu *galben*.

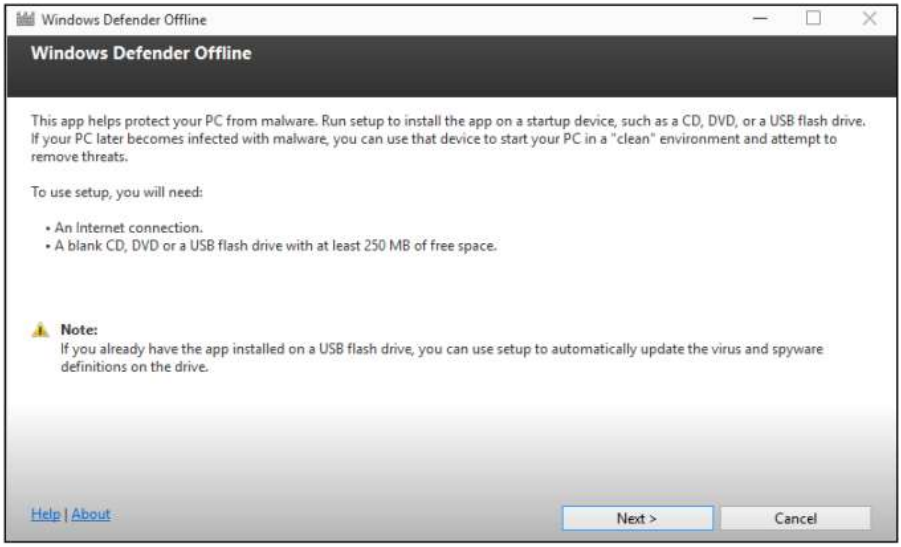
Windows Defender Offline

Dacă atacatorul a reușit să-și infiltreze *rootkiturile* în secvența de boot, iar Windows 7 sau 8.1 nu se mai încarcă, singura posibilitate rămâne utilizarea lui *Windows Defender Offline (WDO)*, distribuit de Microsoft.

În acest caz bootarea se face de pe un CD, DVD sau stick USB, care au un spațiu liber de cel puțin 210MB (pentru versiunea pe 32 biți) sau 230MB (pentru versiunea pe 64 biți).

Windows Defender Offline este o aplicație independentă de sistemul de operare propriu-zis, care verifică prezența *rootkiturilor* în secvența de boot și care poate fi descărcată de pe site-ul *windows.microsoft.com/en-us/windows/what-is-windows-defender-offline*, atât în versiunea de 32 biți, cât și în cea de 64 biți.

După ce ați descărcat versiunea de WDO de care aveți nevoie, creați un CD, DVD sau stick USB bootabile lansând *mssstool32.exe* sau *mssstool64.exe*.



Introduceți CD-ul, DVD-ul sau stickul USB bootabile și restartați Windows 7 sau 8.1. După bootare, lansați WDO și scanați computerul, descoperind *rootkiturile* și *malware*-urile. După ce ați înlăturat toate amenințările software, îndepărtați dispozitivul care conține WDO și restartați computerul în mod obișnuit.



Dacă aveţi instalat Windows 10, nu mai este necesară crearea de suport bootabil cu Windows Defender, deoarece acesta se lansează automat la bootare dacă sesizează malware-uri sau rootkit-uri în secvenţa de boot. Puteţi totuşi crea acest suport bootabile, dar el va fi valabil doar pentru testarea curentă, deoarece baza de date cu semnăturile virușilor nu va mai fi actualizată ulterior.

În cazul nostru am creat un CD boot-abil și pentru Windows 10, cu *msssstool64.exe*, apoi am lansat *Windows Defender Offline*, cu opțiunea de scanare *Full*. În urma scanării au fost detectate amenințările următoare:

- *BrowserModifier:Win32/SupTab*, nivel de amenințare *High*;
- *Trojan:Win32/Bulta!rfn*, nivel de amenințare *Severe*.

WDO a izolat cele două amenințări în *carantină* (Quarantine), apoi au fost eliminate definitiv cu opțiunea *Remove All*.

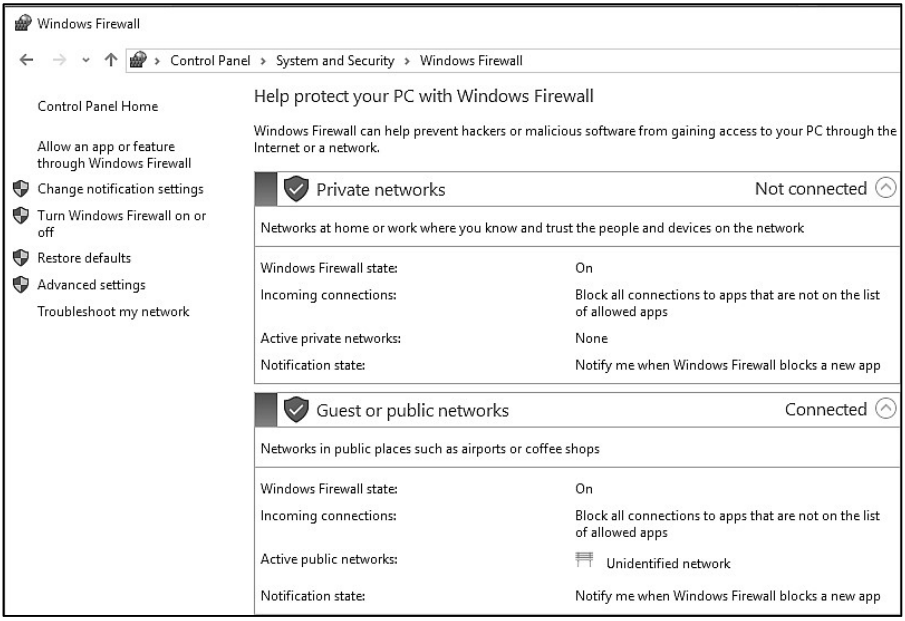
Microsoft susține că *Windows Defender* (atât online, cât și offline) este o aplicație *antivirus*, *antimalware* și *antirootkit* rapidă și eficientă, care elimină necesitatea achiziționării unui antivirus suplimentar.

Windows Defender din Windows 10 este construit pe structura lui *Microsoft Security Essentials*, cu îmbunătățiri în ceea ce privește bootarea securizată (secure boot) cu UEFI, așa că nu are sens să instalați *Microsoft Security Essentials* pe un computer cu Windows 10.

Windows Firewall

Prin activarea lui *Windows Firewall* (WF) se împiedică *accesul neautorizat* al unor persoane sau al unor aplicații externe la sistemul de operare și la fișierele utilizatorului, atunci când acesta lucrează într-o *rețea locală* sau pe *Internet* (cablu sau wireless), permițând browserelor să funcționeze normal.

Pentru a accesa Windows Firewall, tastați *Firewall* în căsuța de căutare pentru Cortana și selectați *Windows Firewall (Control Panel)* sau dați click drept pe *Start*, apoi selectați *Control Panel – System and Security – Windows Firewall*.



Dacă fereastra nu arată ca cea de mai sus (*Private networks* și *Guest or public networks* sunt bifate cu verde), atunci apăsați butonul *Use recommended settings*.

Aplicațille care pot trece de firewall pot fi stabilite cu opțiunea din stânga *Allow an app or feature through Windows Firewall*.

Windows Firewall poate fi oprit selectând *Turn Windows Firewall on or off*.

În cazul în care ați făcut mai multe modificări ale setărilor, puteți reveni la setările implicite selectând *Restore Defaults*.

Setările avansate pot fi accesate cu opțiunea *Advanced settings*.



Windows Firewall poate fi de două tipuri: *inbound* (controlează datele care vin dinspre Internet – cel mai utilizat) sau *outbound* (controlează datele care pleacă de pe PC spre Internet). Setările corespunzătoare celor două tipuri de WF se stabilesc cu opțiunile *Inbound Rules* și *Outbound Rules* din stânga-sus.

Există și firewall de tip *hardware*, încorporat în *routere* sau în *punctele de acces wireless* (WAP – Wireless Access Points). Acestea utilizează un sistem de *translatare a adreselor* (NAT – Network Address Translation), care le creează dificultăți atacatorilor din exterior.

Metode suplimentare de sporire a securității

- *RoboForm* – manager de parole locale sau în cloud, prin criptare cu AES-256;
- *LastPass* – manager de credențiale în cloud, pe servere LastPass;
- *Secunia Personal Software Inspector* – asigură update-uri pentru toate aplicațiile;
- *NoScript add-on for Firefox* – blochează Java, Flash și Adobe Acrobat Reader.
- *VyprVPN* – permite deschiderea unui tunel VPN criptat într-o rețea wireless.

Iată câteva dintre facilitățile oferite de *RoboForm*: Password Manager, Password Generator, Password Sync, Form Filter, Start Page și Search Box.

Rețele

Îmbunătățiri aduse rețelelor wireless
Wi-Fi Sense
Conectarea prin VPN Wi-Fi
Power Shell
Remote Desktop
Suport pentru IPv6

Îmbunătățiri aduse rețelelor wireless

Cea mai importantă îmbunătățire introdusă de Windows 10 este noua *interfață pentru driverurile wireless* (WDI – Wireless Driver Interface), care este funcțională atât pentru *PC*-uri cât și pentru *dispozitivele mobile* (tablete sau smartphone-uri).

Unul din cele mai importante beneficii ale WDI este *administrarea conexiunilor utilizând același tip de manager* (stack) și *readucerea rapidă în stare de funcționare* a echipamentelor care se blochează din considerente firmware.

Noul driver suportă, de asemenea, *randomizarea adreselor MAC (Media Access Control)*, îmbunătățind securitatea și intimitatea utilizatorilor.

Și dispozitivele *bluetooth* au fost îmbunătățite, atât cele *clasice*, cât și cele cu *consum energetic redus* (low energy), cu suport audio pentru *convorbiri pe bandă largă* sau prin *codecuri aptX*, ce egalează în calitate transmisia audio pe fir.

Dacă este necesară o securitate maximă, prin funcția de *limitare a domeniului de conectare wireless* (SSP – Simple Secure Pairing), se pot accepta doar conexiunile wireless ale mouse-urilor și tastaturilor, reducând astfel posibilitatea atacurilor din exterior.

Începând cu Windows 8.1 au fost introduse trei *standarde wireless*, care au fost îmbunătățite în mod substanțial în Windows 10:

• ***Near Field Communication (NFC)*** Windows 8.1 a introdus împerecherea echipamentelor prin simpla apropiere și atingere a acestora (*tap-to-pair*). Astfel, un dispozitiv mobil poate fi conectat la imprimanta care suportă NFC a unei instituții prin simpla atingere a celor două echipamente.

Windows 10 Mobile a transformat smartphone-urile în cărți de credit virtuale, prin adăugarea suportului *HCE* (*Host Card Emulation)*, alături de clasicul element de securitate *UICC (Universal Integrated Circuit Card*), plata cumpărăturilor putând fi efectuată prin simpla atingere a casei de marcat cu smartphone-ul. Pot exista chiar *mai multe HCE-uri pe același smartphone*.

Două *smartphone*-uri sau *tablete* pot comunica între ele prin simpla atingere a acestora, dacă suportă standardul *NFC*.

• ***Wi-Fi Direct*** Acesta este un standard relativ nou, care le permite dispozitivelor să se conecteze între ele, într-o rețea wireless, două câte două, fără necesitatea existenței unui *punct de acces* (access point). Conectarea se face automat, fără intervenția expresă a utilizatorului.

Tehnologia permite *conectarea la echipamentele* unei instituții (imprimante, scannere etc.), *fără instalarea unor drivere sau softuri dedicate*.

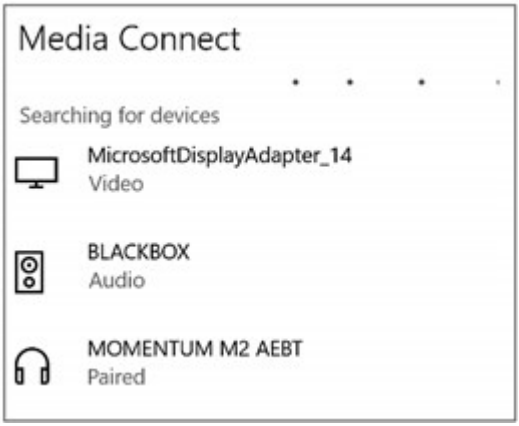
• ***Miracast Wireless Display (MWD).*** Este un alt standard care utilizează *Wi-Fi Direct* pentru a transmite *stream-uri audio sau video* către *display*-urile sau *proiectoarele* care suportă *Miracast*.

Toate echipamentele care au instalat Windows 10 suportă *Miracast*, permiţând posesorilor de *tablete* şi *laptopuri* să susţină o conferinţă pe un *proiector cu Miracast*, fără a utiliza cabluri sau adaptoare specializate (dongles).

Adaptorul wireless pentru display al lui Microsoft (*Miracast Wireless Display Adapter*), poate fi conectat pe intrarea *HDMI* a unui TV cu diagonală mare sau pe o tablă electronică, *fără a fi necesară vreo setare*.

Multe din aceste conexiuni pot fi efectuate apăsând tile-ul *Connect*, aflat în partea inferioară a lui Action Center, sub partea de notificări.

Figura de mai jos exemplifică o conexiune de afişare prin *Microsoft Wireless Display Adapter*, o conexiune *Bluetooth* către o pereche de boxe audio şi o conexiune audio *Bluetooth* către o pereche de căşti.



Autorul utilizează o conexiune prin *Bluetooth* între *laptop* şi un *sistem audio 2+1*, conexiunea realizându-se în mod automat la fiecare pornire a laptopului.

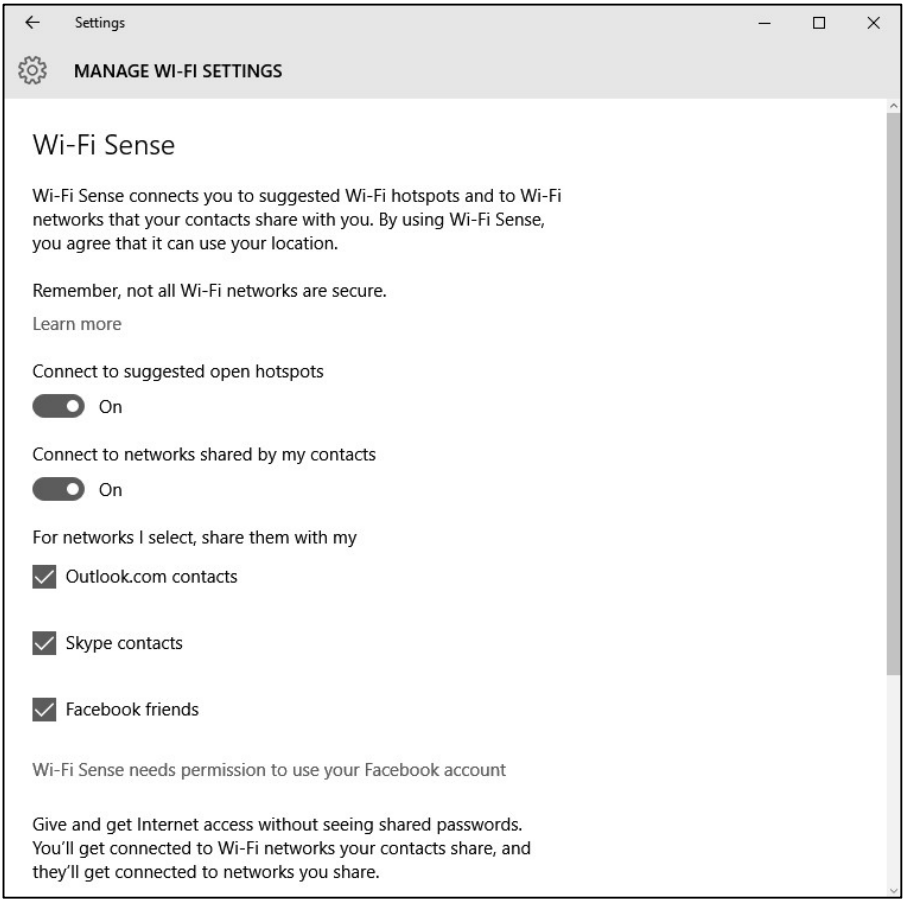
Dispozitivele conectate prin *Miracast* le puteţi găsi urmând calea *Start – Settings – Devices – Connected Devices*. Pentru a adăuga un dispozitiv nou, apăsaţi *Add a device* din secţiunea *Add devices*.

Setările pentru *MWD* pot fi efectuate cu *Start – All apps – Wireless Display Adapter*.

Miracast este suportat şi de *smartphone*-urile cu *Android 4.2* sau *mai recent*.

Wi-Fi Sense

Pentru a avea acces la opţiunile *Wi-Fi Sense*, urmaţi calea *Start – Settings – Network & Internet – Wi-Fi – Manage Wi-Fi Settings*.



Prin *Wi-Fi Sense* puteţi avea o conexiune sigură, printr-un *spot wireless* aflat acasă, într-un mall sau într-o cafenea, la mail-urile din *Outlook.com*, la contactele din *Skype* şi la prietenii de pe *Facebook*. Wi-Fi Sense *nu suportă reţelele 802.1x* şi utilizează poziţia în care vă aflaţi (*Location*).

Conectarea prin VPN Wi-Fi

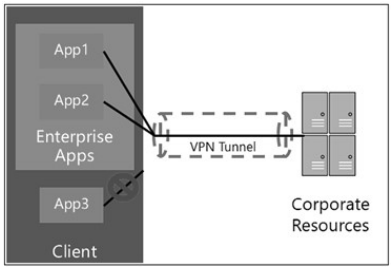
Dacă un angajat al unei instituții vrea să se conecteze printr-un *hotspot Wi-Fi* la rețeaua locală a acesteia, conexiunea poate fi interceptată de un atacator, provocând daune devastatoare pentru instituția respectivă.

Soluția constă în utilizarea unei *conexiuni virtuale private* (VPN – Virtual Private Network), care este criptată și nu poate fi interceptată de către un atacator din exterior.

Windows 8 a inclus un *client Microsoft VPN* de bază, iar Windows 8.1 a adăugat suport pentru o *selecție limitată de furnizori VPN* (Check Point, F5, Juniper Networks și SonicWall).

Windows 10 extinde soluțiile VPN, utilizând conexiuni private prin *Store*, care devin în mod automat *VPN*-uri atunci când Windows 10 sesizează încercarea de accesare prin wireless a intranetului unei instituții.

Dacă angajatul accesează în permanență intranetul respectiv, atunci se poate seta ca sesiunea VPN să devină *permanentă*.



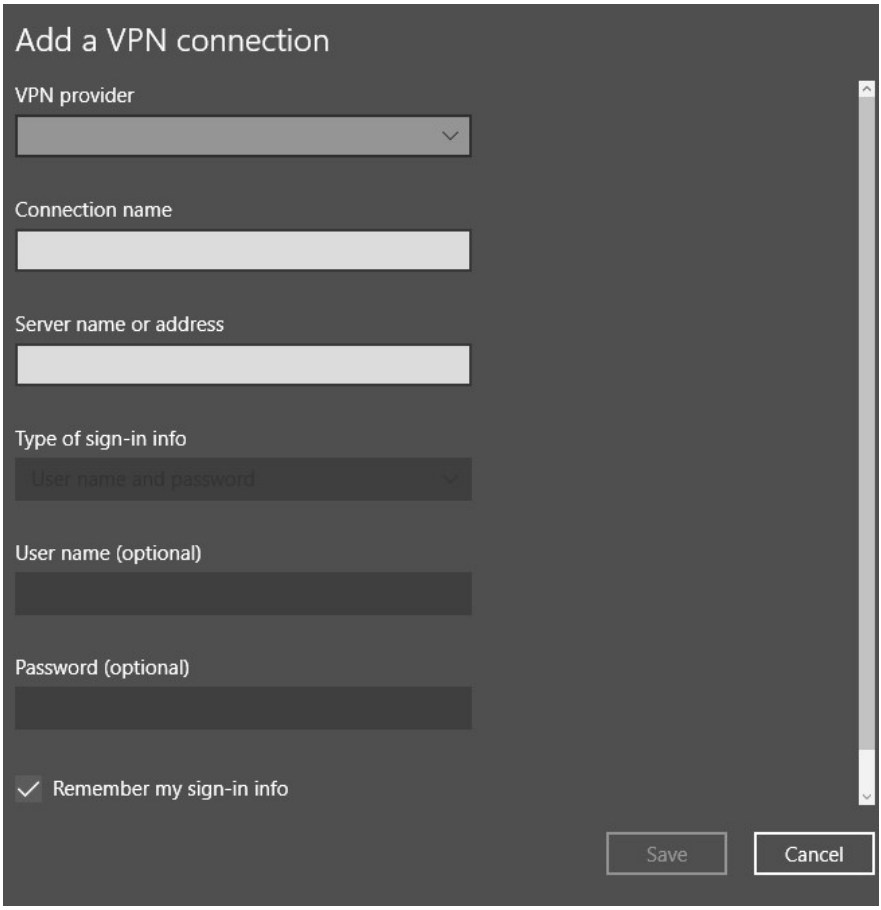
Administratorii de rețea pot crea o *listă* a *utilizatorilor* sau a *aplicațiilor* care pot accesa rețeaua locală prin VPN, blocând restul încercărilor de acces.

Pentru a deschide o conexiune VPN se urmează calea *Start – Settings – Network & Internet – VPN – Add a VPN Connection*.

În fereastra care se deschide (vezi pagina următoare) se selectează provider-ul de Internet (*Check Point Capsule VPN, F5 VPN, SonicWall Mobile Connect* sau *Windows built-in),* se introduce numele conexiunii (*VPN Serviciu*), numele serverului (*ex.mydomain.local),* se selectează tipul de VPN (*Automatic, Point to Point Tunneling – PTP, Layer 2 Tunneling with IPsec – L2TP/IPsec, Secure Socket Tunneling Protocol – SSTP sau IKEv2,* se aleg tipurile de credențiale (*User name and Password, Smart card* sau *One-time password*), se introduce *numele utilizatorului* și *parola* (dacă s-a ales prima variantă), apoi se apasă butonul *Save.*

Veți observa că în secțiunea *VPN* a ferestrei *Network & Internet* a apărut conexiunea *VPN Serviciu*. Se dă clic pe conexiune, apoi pe *Connect*.

Setările avansate ale conexiunii *VPN Serviciu* se pot face apăsând butonul *Advanced Options* și apoi *Connect*.



Pentru a întări securitatea conexiunilor VPN prin Wi-Fi, se poate utiliza facilitatea *DirectAccess*, ce necesită un client pe care este instalat *Windows 10 Enterprise* și un server *Windows Server 2012, 2012 R2* sau *2016*.

DirectAccess le permite utilizatorilor de echipamente *mobile* să acceseze în siguranță, prin Wi-Fi, resursele instituției.

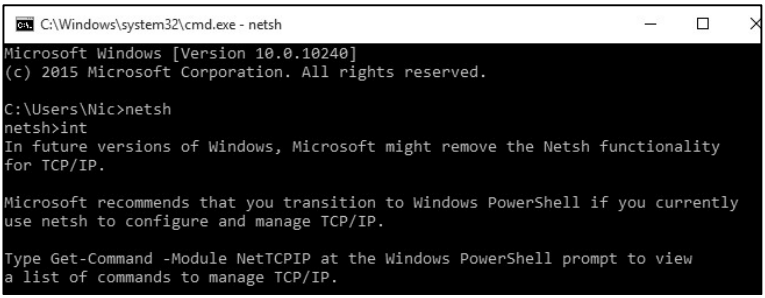
Pentru a apela *DirectAccess* se urmează calea *Start – Settings – Network & Internet – DirectAccess*.

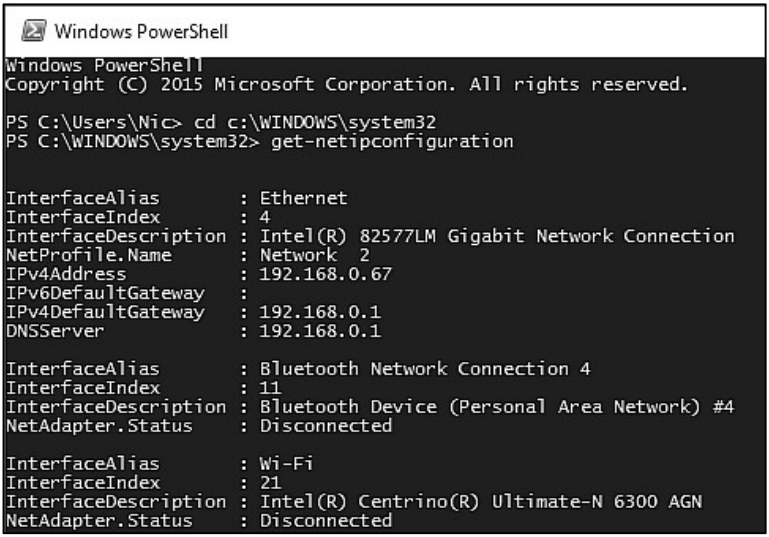
Power Shell

Power Shell din Windows 10 este mult mai puternic decât *Command Prompt*, în ceea ce privește administrarea rețelelor. Tastați *power* în căsuța de căutare pentru Cortana și selectați *Windows PowerShell (Desktop app)*.

Comenzile din PowerShell se numesc *cmdlets* și puteți găsi o listă completă a acestora la adresa *https://technet.microsoft.com/en-us/library/hh849695.aspx*.

Dacă veți tasta *netsh*, apoi *int* în fereastra *Command Prompt*, veți obține mesajul de mai jos, adică o trimitere clară spre *PowerShell* și spre comanda *get-netipconfiguration*, unde veți obține un rezultat foarte detaliat al conexiunilor.

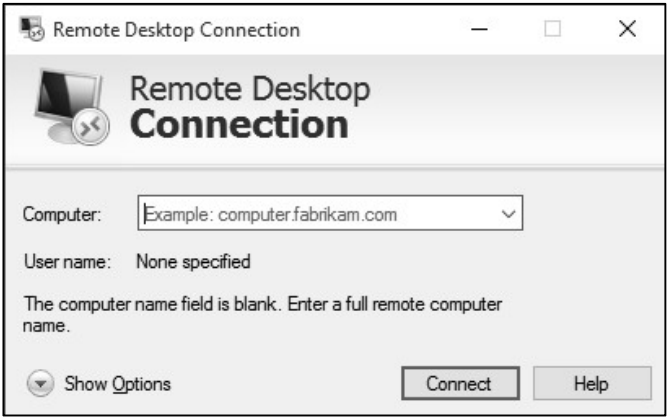




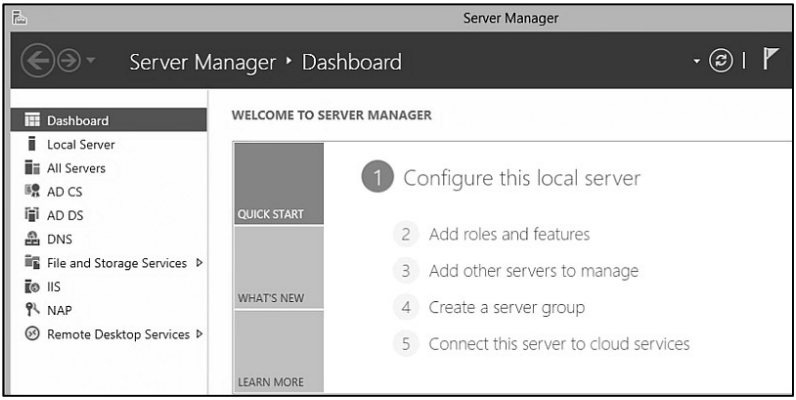
Remote Desktop

O facilitate binecunoscută din versiunile anterioare de Windows, utilizată pentru a acesa de la distanță anumite resurse, este *Remote Desktop*.

Pentru a lansa Remote Desktop, tastați *remote* în căsuța de căutare pentru Cortana și selectați *Remote Desktop Connection (Desktop app*).



Introduceți *numele* sau *IP*-ul computerului / serverului pe care vreți să-l accesați de la distanță, apoi tastați *parola* cu care vă conectați în modul local. În cazul nostru a fost accesat de la distanță un server cu *Windows Server 2012*.



Windows 10 are și o versiune universală de *Remote Desktop*, care poate fi descărcată din *Windows Store* și care poate fi utilizată atât pe *PC* sau *laptop*, cât și pe *2-in-one*, *tabletă* sau *smartphone*.

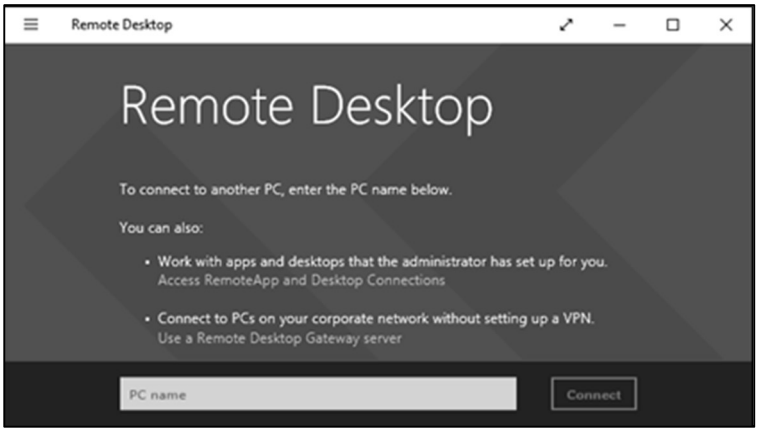
Pentru a descărca și instala aplicația, deschideți mai întâi *Store* și, în căsuța de căutare *Search*, din dreapta sus, tastați *remote*, apoi alegeți *Remote Desktop (Apps and Games)*. Pentru instalare apăsați butonul *Free*. Aplicația este descărcată în mod automat, iar după instalare, butonul *Free* se va schimba în *Open*.

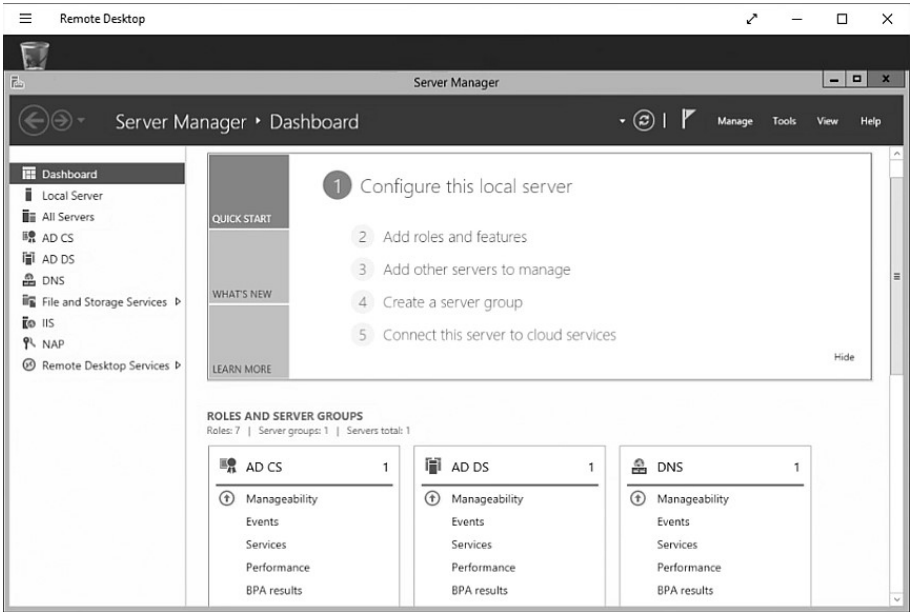


Pentru a deschide aplicația, urmați calea *Start – All Apps – Remote Desktop* și se va deschide fereastra *Remote Desktop* (vezi pagina următoare).

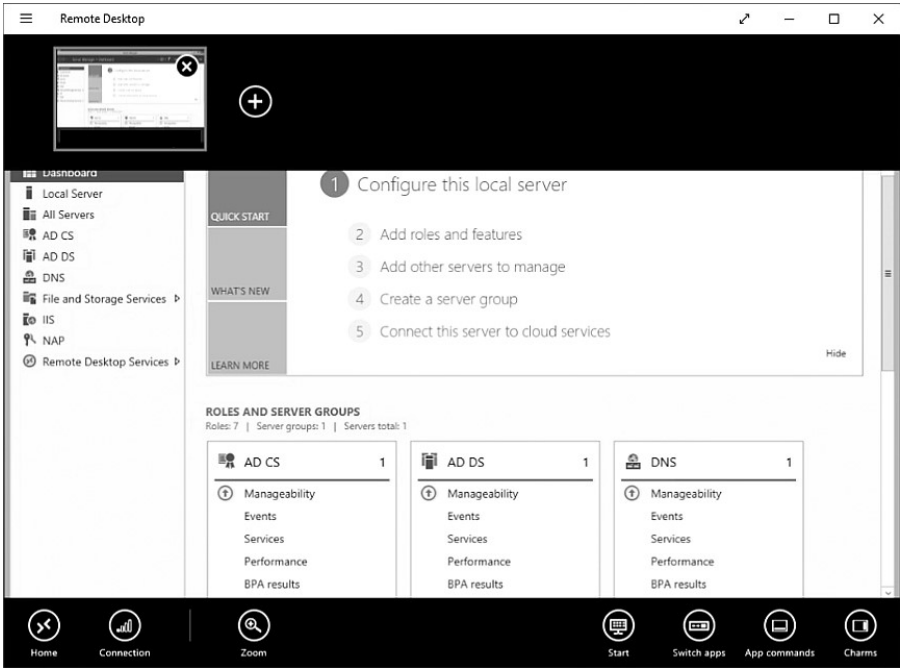
Prin intermediul acestei aplicații puteți lucra de la distanță cu aplicații și desktop-uri pe care administratorul le-a setat pentru dumneavoastră (*Access RemoteApp and Desktop Connections*) sau vă puteți conecta la rețeaua de la serviciu, printr-un server gateway (*Use a Remote Desktop Gateway Server*).

În căsuța *PC Name* se poate introduce *IP*-ul computerului care se dorește a fi accesat de la distanță sau *numele de domeniu* al acestuia. Dacă ați introdus numele serverului accesat anterior prin aplicația clasică *Remote Desktop*, veți obține o fereastră aproape identică, dar cu facilități suplimentare.





Astfel, dacă vom da un clic pe bara superioară de deasupra titlului *Server Manager*, în centrul acesteia va apărea *numele serverului*, iar în partea inferioară vor apărea *şapte butoane circulare*, cu diverse funcţionalităţi.



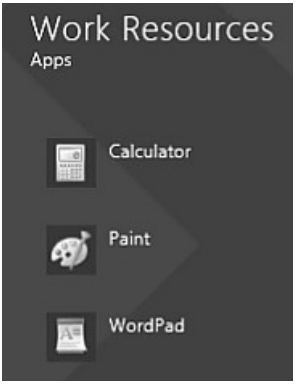
Deoarece fereastra *Remote Desktop* nu poate fi redimensionată, butonul *Zoom* vă ajută să măriți fonturile din interiorul acesteia, apoi puteți utiliza *bara de scroll* pentru deplasare în interior.

Se poate adăuga o *conexiune suplimentară*, apăsând butonul ⊕ din stânga-sus. În acest fel se pot monitoriza de la distanță mai multe computere simultan.

Dacă apăsați butonul ☰ din colțul din stânga sus al ferestrei și selectați *Settings – Connection Settings*, puteți efectua setări amănunțite ale modului în care doriți să apară fereastra respectivă.

Dacă urmați calea ☰ *– Settings – Manage Remote App and desktops*, atunci veți putea deschide conexiuni către *aplicațiile* sau *desktopurile* la care administratorul v-a oferit posibilitatea accesului de la distanță.

Selectați *Add a new connection*, introduceți *numele* sau *IP*-ul computerului, apăsați butonul *Connect,* apoi introduceți *numele utilizatorului* și *parola*. Veți primi un mesaj în care sunteți informați de numărul desktop-urilor și aplicațiilor pe care le puteți acccesa (de exemplu *2 desktops, 3 apps*), la care tastați *OK*.



Apare o nouă fereastră *Remote Desktop* în care puteți să selectați aplicația cu care doriți să lucrați (de exemplu *Paint*). Apăsați butonul *Connect* în fereastra *RemoteApp* care apare. Trebuie remarcat că aplicația *Paint* va rula pe desktopul local și nu în interiorul ferestrei *Remote Desktop*.

Suport pentru IPv6

Tranziția de la *IPv4* la *IPv6* a fost propusă cu mulți ani în urmă, dar nu a fost realizată încă, deși spațiul de adrese utilizat de IPv4 riscă să devină insuficient.

Utilizarea *translatării adreselor* (NAT – Network Address Translation) le permite utilizatorilor din rețelele mici și mijlocii să *partajeze* o singură *adresă IPv4* de Internet, dar acest lucru duce la o încetinire a serviciilor care se bazează pe o comunicație directă.

Pentru *Windows 10 IoT* problema a devenint și mai acută, deoarce acesta se bazează doar pe comunicații directe între două echipamente.

Dacă *IPv4* oferă un spațiu de adrese de $4{,}3\times10^{9}$, spațiul de adrese oferit de *IPv6* este incredibil de mare: $3{,}4\times10^{38}$. În afară de spațiul de adrese extins, IPv6 oferi noi facilități de îmbunătățire a securității echipamentelor, precum *IPsec*, care asigură *securitatea la nivel de pachet*.

Pe durata tranziției de la IPv4 la IPv6 vor fi implementate topologiile *dual-stack*, care le vor permite echipamentelor să fie configurate atât cu IPv6, cât și cu IPv4. Începând cu Windows 8, se acordă *prioritate* lui *IPv6 față de IPv4*. Pentru aplicațiile care *nu suportă IPv6*, Windows va selecta în mod *automat* sistemul *IPv4*, procedură cunoscută sub denumirea de *address sorting* (sortarea adreselor).

Windows Server 2012 R2 extinde suportul pentru IPv6 în *Group Policy* și permite efectuarea noilor tipuri de setări pe stațiile care rulează *Windows 8.1* sau *mai recent*.

Principalele *facilități* oferite de *Windows Server 2012 R2* sunt următoarele:

- Configurarea *imprimantelor* prin TCP/IP versiunea *IPv6*;
- În Group Policy se poate seta o *adresă IPv6* în locul unui *interval de adrese IPv4*.
- Pentru conexiunile *VPN*, este recomandabilă bifarea căsuței *Use IPv6*.

Mai multe detalii despre aceste *setări* puteți obține la linkul următor: *http://technet.microsoft.com/en-us/library/dn265973.aspx*.

Virtualizare

Mașini virtuale
Client Hyper-V
Virtualizarea desktop-urilor
Virtualizarea aplicațiilor
UE-V

Mașini virtuale

Cu *Windows 10 Pro* și *Enterprise* pe 64 de biți se pot crea *mașini virtuale* (VM – Virtual Machines) în care să ruleze *copii de Windows, ediții diferite* ale aceleiași versiuni de Windows sau *sisteme de operare diferite*, utilizând același *hypervisor* din sistemele *Windows Server*.

Mașinile virtuale sunt foarte utile în următoarele cazuri:

• Aveți pe CD-uri sau DVD-uri *aplicații* care rulează doar sub *versiuni anterioare de Windows* (XP, 98, 95 etc.). Pentru a putea rula aceste aplicații și sub Windows 10, creați o *mașină virtuală* în care instalați vechiul sistem de operare sub care rulează aplicația, apoi instalați *aplicația* în mașina virtuală nou creată. Dacă vechea aplicație necesită și *conexiune la Internet*, atunci îi puteți atașa o *placă de rețea virtuală* (virtual network interface card).

• Vreți să faceți un studiu comparativ despre mai multe *sisteme de operare* (Microsoft Windows, Linux, Novell Netware, Sun Solaris etc.) și aveți nevoie să fie funcționale simultan. Creați câte-o *mașină virtuală* pentru fiecare sistem de operare, instalați *sistemul de operare* și *salvați* mașina virtuală respectivă. Dacă vreți să accesați un anumit sistem de operare, alegeți mașina virtuală dorită din lista VM-urilor create.

• La fel veți proceda dacă vreți să faceți un studiu comparativ despre *versiuni ale lui Microsoft Windows* (de exemplu Vista, Windows 7, Windows 8 și Windows 10) sau despre *versiuni ale serverelor Microsoft* cu *Active Directory* (2000, 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 și 2016).

• Vreți să faceți *experimente riscante* cu Windows 10, care pot duce la *virusarea* sistemului de operare sau la *modificarea nedorită a regiștrilor*. Creați o *mașină virtuală* și *instalați Windows 10* în aceasta, apoi începeți *experimentul*. Chiar dacă Windows 10 din mașina virtuală se va virusa sau regiștrii vor suferi modificări importante, Windows 10 original nu va fi afectat.

O mașină virtuală are alocat un anumit *spațiu de memorie* în care poate să ruleze (*Hyper-V* necesită 2GB – 4GB), de aceea nu este recomandabil să creați mașini virtuale pe computere care au *4GB de RAM sau mai puțin*, deoarece performanțele sistemului de operare original pot scădea în mod drastic.

În rețelele complexe, administratorii pot utiliza *unelte de virtualizare de tip server* (server-based virtualization tools) pentru a oferi accesul clienților la *aplicații* sau chiar la *desktop*-uri integrale.

Client Hyper-V

Deşi au existat aplicaţii pentru virtualizare şi în versiunile anterioare de Windows (VirtualPC), *Client Hyper*-V a fost introdus de către *Windows 8*.

Client *Hyper-V* din *Windows 10 Pro* şi *Enterprise* pe 64 de biţi utilizează aceaşi tehnologie şi aceleaşi formate pe care le utilizează *Windows Server*. Sistemele de operare din maşina virtuală (pe *32 de biţi* sau pe *64 de biţi*), pot fi instalate de pe un *mediu fizic* (CD sau DVD) sau prin montarea unei *imagini ISO*.

Există şi posibilitatea creării unui *hard disk virtual* (VHD – virtual hard disk) dintr-un hard disk fizic, care conţine deja sistemul de operare, utilizând *Windows Sysinternals Disk2vhd Tool*. Pentru detalii accesaţi următorul link:

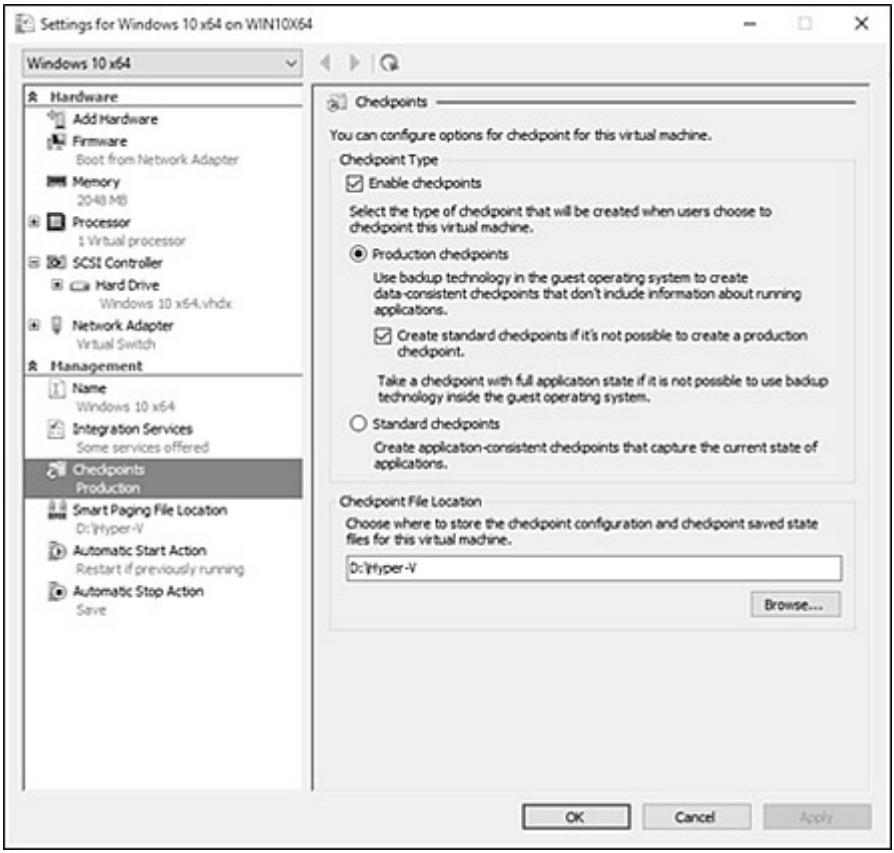
https://technet.microsoft.com/en-US/sysinternals/ ee656415

Utilizând *Virtual Machine Manager* din System Center, în reţelele complexe se pot converti *computere fizice* în *maşini virtuale:* (P2V - How to Deploy a Virtual Machine by Converting a Physical Computer). Mai multe detalii găsiţi aici:

https://technet.microsoft.com/en-US/library/hh368990.aspx

În ceea ce priveşte *managementul* pentru *Client Hyper-V*, Windows 10 a adăugat câteva *facilităţi* importante:

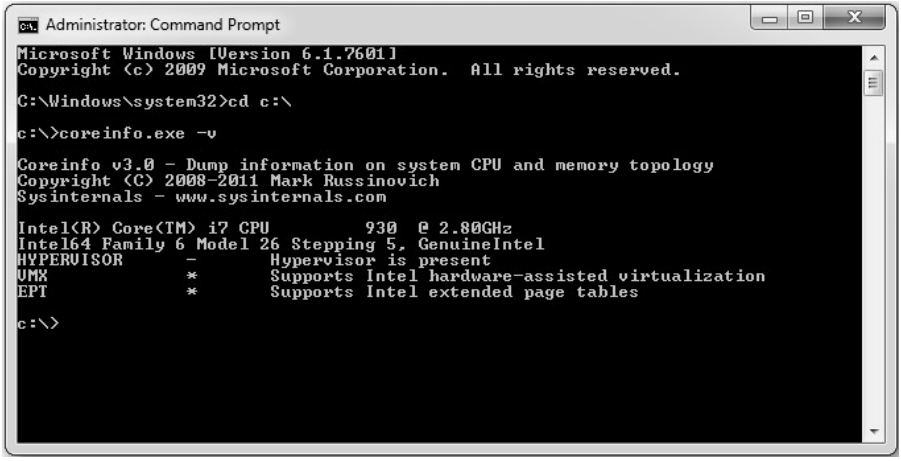
- ***Puncte de control ale productivităţii*** *(production checkpoints)*. Prin utilizarea lui *Volume Snaphot Service* se pot crea *puncte de verificare* (point in time backups), care pot fi restaurate foarte uşor (vezi secţiunea *Checkpoints*, care apare în *Hyper-V Manager* atunci când o maşină virtuală este activă: clic drept pe VM – *Checkpoint*).
- ***Noi formate ale fişierelor de configurare.*** Vechiul format de fişiere ***.****XML* a fost abandonat în favoarea formatelor *.VCMX* (pentru datele de configurare ale maşinilor virtuale) şi *.VRMS* (pentru datele despre starea execuţiei).
- ***Modificarea memoriei şi a adaptorului de reţea în timpul rulării VM.*** *Spaţiul de memorie* alocat unei maşini virtuale poate fi modificat *în timpul funcţionării* acesteia, chiar dacă nu este activat *Dynamic Memory*, atât la maşinile virtuale din generaţia 1, cât şi la cele din generaţia a 2-a. Pe acestea din urmă se poate chiar adăuga sau elimina *adaptorul de reţea* în timpul rulării VM.
- ***Compatibilitate Connected Standby.*** Când este activat Hyper-V pe un computer care utilizează modelul *Always On/Always Connected (AOAC)*, aşa cum este *Microsoft Surface 3*, starea *Connected Standby* (conectare la reţea cu consum energetic minim) este, de asemenea, disponibilă.
- ***Îmbunătăţiri ale managerului Hyper-V.*** Deşi este concepută să lucreze cu Windows Server 2016, consola *Hyper-V Management* din Windows 10 include managementul *serverelor de nivel inferior*, aşa cum este Windows Server 2012, şi permite utilizarea *credenţialelor alternative* pe un server sau computer aflate la distanţă.

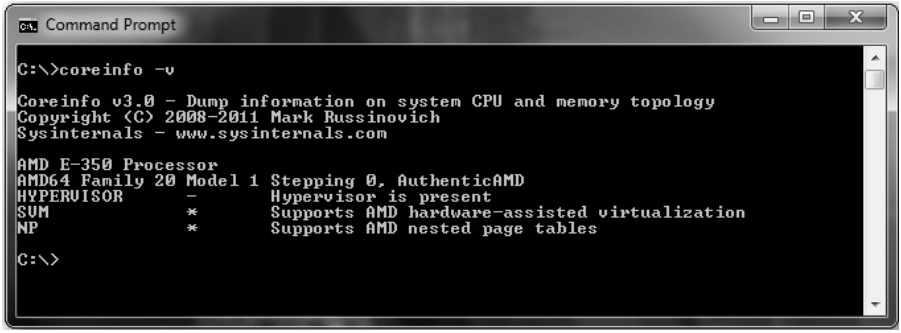


Pentru a crea și rula *mașini virtuale* pe computerele cu *Windows 10 Pro și Enterprise* pe *64 de biți*, acestea trebuie să aibă activată și opțiunea de *translatare a adreselor la nivel secundar* (Second Level Address Translation – SLAT). Pentru a verifica dacă SLAT este disponibil pe computerul dumneavoastră, accesați linkul *www.howtogeek.com/73318/how-to-check-if-your-cpu-supports-second-level-address-translation-slat*, descărcați și instalați aplicația *CoreInfo*, apoi executați sub *Command Prompt*, ca administrator, comanda *coreinfo –v*.

SLAT este disponibil pe computerele cu procesoare *Intel*, dacă în rândul EPT este un *asterisc*, iar dacă procesorul este *AMD*, asteriscul este în rândul NP/NPT.

Dacă în loc de asterisc este o *liniuță*, atunci procesorul nu suportă *SLAT*.



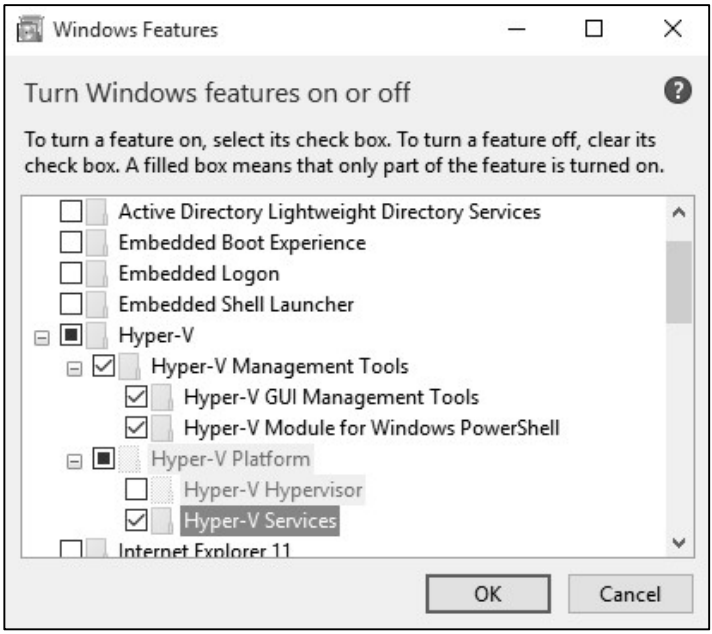


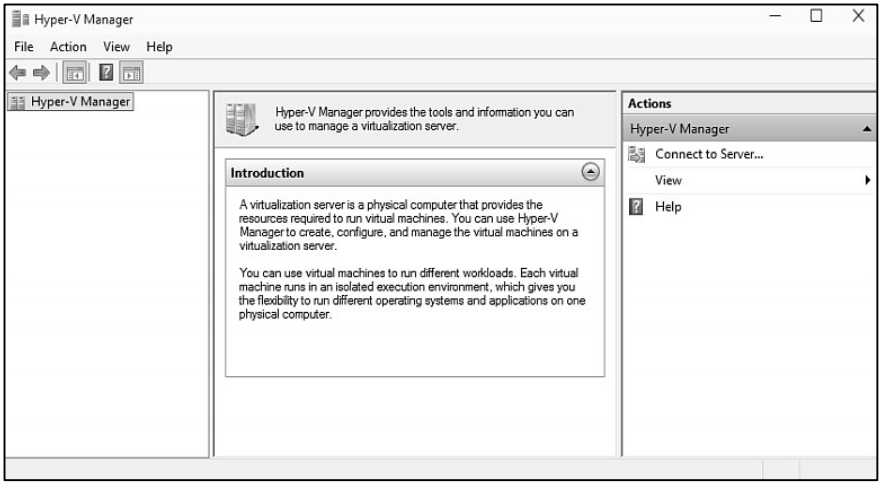
Activarea clientului *Hyper-V* se fac urmând calea*:* clic drept pe *Start – Control Panel – All Control Panel Items – Programs and Features – Turn Windows features on and off* (stânga-sus) – expandare *Hyper-V* – bifare componente Hyper-V pe care doriți să le utilizați – *OK* (Windows instalează *Hyper-V Manager* și *Hyper-V Virtual Machine Connection*) – *Start – Power – Restart*.

Clientul *Hyper-V* poate fi activat și printr-un *cmdlet* în *PowerShell*:

…>Enable-WindowsOptionalFeature-Online-FeatureName Microsoft-Hyper-V

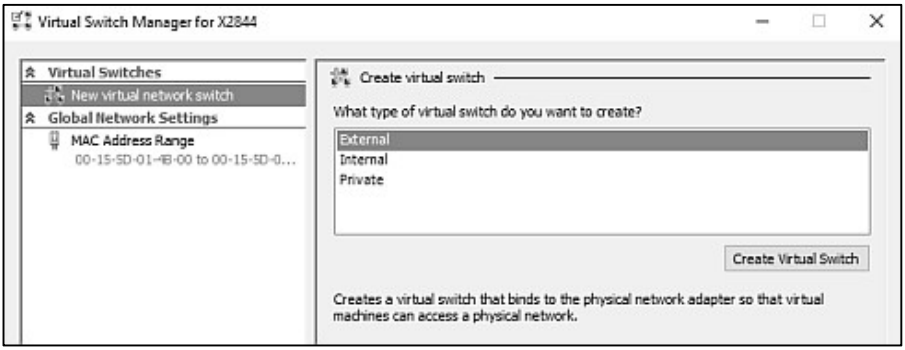
După repornirea computerului, crearea mașinilor virtuale se face utilizând wizard-ul din *Hyper-V Manager* sau prin modulul Hyper-V din *PowerShell*.


Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Active Directory Lightweight Directory Services
Embedded Boot Experience
Embedded Logon
Embedded Shell Launcher
Hyper-V
Hyper-V Management Tools
Hyper-V GUI Management Tools
Hyper-V Module for Windows PowerShell
Hyper-V Platform
Hyper-V Hypervisor
Hyper-V Services
Internet Explorer 11
OK
Cancel


Hyper-V Manager
File Action View Help
Hyper-V Manager
Hyper-V Manager provides the tools and information you can use to manage a virtualization server.
Introduction
A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server.
You can use virtual machines to run different workloads. Each virtual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer.
Actions
Hyper-V Manager
Connect to Server...
View
Help

Pentru a crea o mașină virtuală, urmați calea *Start – All Apps – Hyper-V Management Tools – Hyper-V Manager*. În secțiunea *Actions* din dreapta ferestrei Hyper-V Manager selectați *Connect to Server*, dați clic pe butonul *Local Computer* și apoi pe butonul *OK*.

Pentru a crea o *conexiune de Internet* pentru *mașina virtuală*, trebuie creat mai întâi un *switch virtual* (virtual switch). Tot în secțiunea *Actions* selectați acum *Virtual Switch Manager*. În lista derulantă care apare în fereastra *Create virtual switch* selectați *External*, apoi apăsați butonul *Create Virtual Switch*.



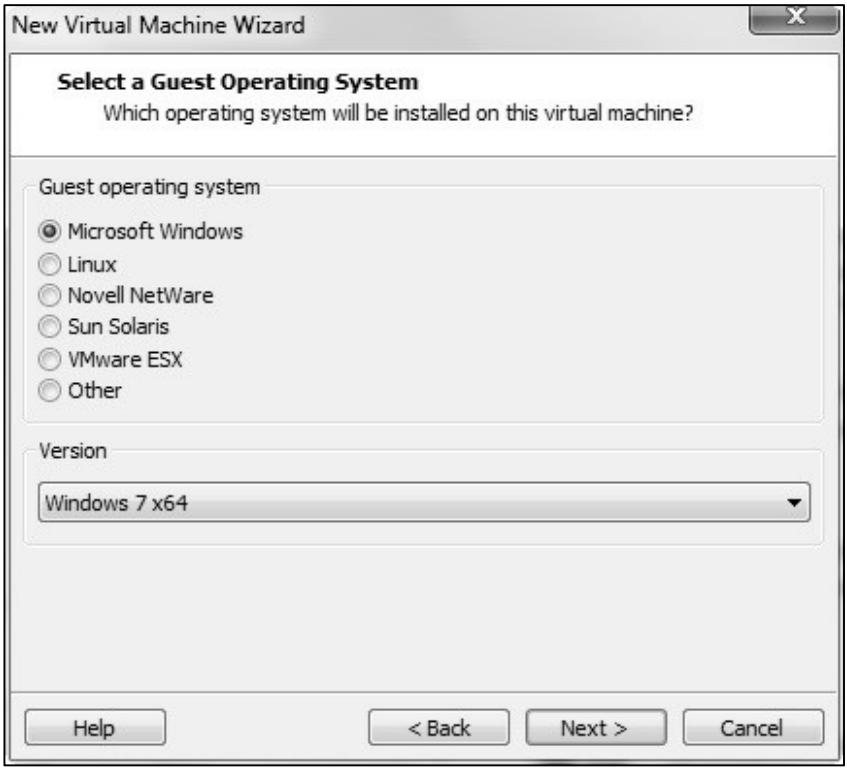
În fereastra *Virtual Switch Properties*, introduceți un *nume* pentru switch-ul virtual în căsuța *Name*, lăsați neschimbate celelalte setări, apoi apăsați butonul *OK*. Veți fi redirecționați către fereastra *Hyper-V Manager*.

În aceeași secțiune *Actions*, selectați *New*, apoi *Virtual Machine*, prin care va fi lansat wizard-ul *New Virtual Machine Wizard* (vezi pagina următoare). Selectați *sistemul de operare* sau *versiunea de Windows* dorite, apoi apăsați butonul *Next*.

În fereastra *Specify Name and Location* care apare, dați un *nume* mașinii virtuale (de exemplu Windows 7 Ultimate x64), apoi specificați *folderul* de pe hard disk care va găzdui mașina virtuală (de exemplu *D:\Masini virtuale\ Windows 7 Ultimate x64*) și apăsați butonul *Next*. Alegeți *Generation 1*, apoi din nou *Next*.

Wizard-ul vă va solicita acum să specificați *spațiul de mem*orie alocat mașinii virtuale. Dacă intenționați să rulați *Windows 7, 8.1 sau 10*, alocați 2048MB și selectați *Use Dynamic Memory for this Virtual Machine box*. Pentru Linux rezervați doar 512MB și nu mai utilizați *Dynamic Memory*.

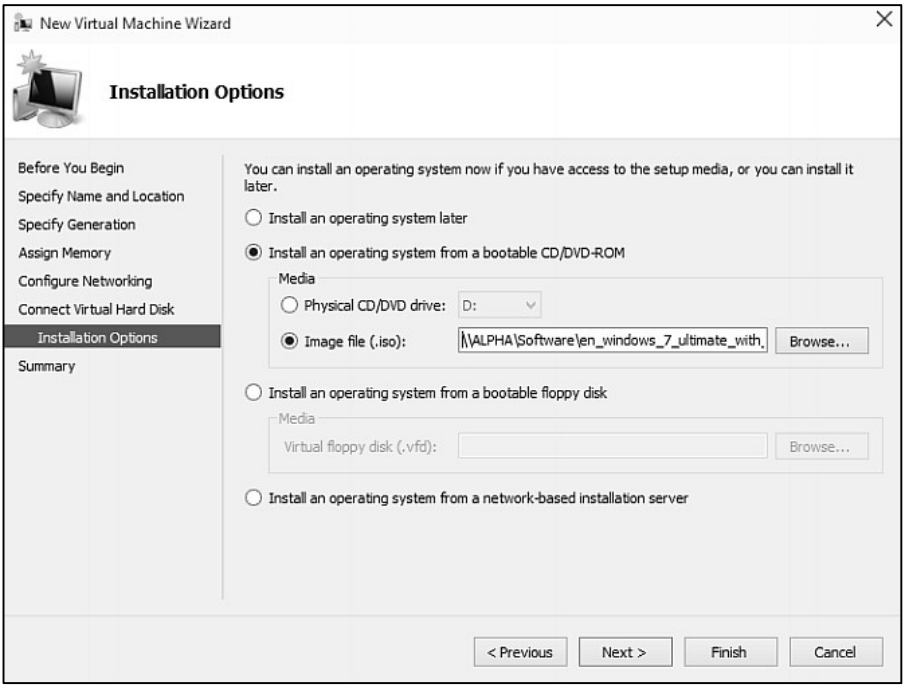
În fereastra *Connection* alegeți *numele conexiunii de Internet* create anterior și alegeți un *nume* pentru hard disk-ul virtual (diferit de cel din *Windows Storage Spaces*), apoi apăsați *Next*.



Pasul final în crearea mașinii virtuale este *instalarea sistemului de operare* dorit. Puteți alege între instalarea de pe un *CD/DVD-ROM bootabile* sau de pe o *imagine ISO*, căreia trebuie să-i specificați *folderul* în care se află. După cum se observă în imaginea din pagina următoare, mai există și opțiunile de instalare de pe un *floppy disk bootabil* (în cazul sistemelor de operare mai vechi) sau de pe un *server de instalare* din rețeaua locală (network-based instalation server).

Apăsați butonul *Next*, iar după instalarea sistemului de operare dorit, apăsați butonul *Finish*. Mașina virtuală nou creată va apărea în partea din stânga-sus a aplicației *Hyper-V Manager*. Pentru lansare, dați *dublu clic* pe mașina virtuală respectivă sau alegeți *Action – Start* din meniul superior al lui *Hyper-V Manager*.

Un control mai flexibil al mașinii virtuale se poate face adăugând Integration Services Setup Disk cu *Action – Insert Integration Services Setup Disk*.



Client Hyper-V mai include suport pentru *CredSSP, Kerberos* și *autentificare NTLM* prin protocol *WS-MAN*.

Cu *Windows PowerShell Direct* se pot executa *cmdlets* în mașinile virtuale instalate. Accesarea mașinilor virtuale într-o sesiune extinsă se poate face cu aplicația *Hyper-V Virtual Machine Connection*, care este o variantă a tehnologiei *Remote Desktop*.

O mașină Hyper-V poate suporta până la *12 monitoare*, cu suport pentru rețele *wireless* și pentru stările *sleep* sau *hibernate*.

Suporturile *audio* și *USB* nu sunt active în mod implicit, dar pot fi activate prin *Remote Desktop*, specificând *resursele locale* ale clientului.

De asemenea, nici facilitatea *multitouch* nu este disponibilă la mașinile virtuale, dar se poate utiliza *single-touch*.

Virtualizarea desktop-urilor

În Windows 10 există posibilitatea utilizării desktop-urilor virtuale pe computerul individual, așa cum au fost descrise în volumul anterior „Windows 10 Ghid practic". În rețea, desktop-urile virtuale sunt oferite clienților prin aplicația *Remote Desktop Services (RDS)*, care rulează pe *Windows Server 2012, Windows Server 2012 R2* și *Windows Server 2016*.

Remote FX utilizează *unitatea de prelucrare grafică* (graphics processing unit – GPU) sau *hardware-ul GPU* de pe server pentru a le furniza clienților desktop-uri cu *grafică 3D* și o experiență *multimedia* complexă.

Prin *FairShare* se asigură o performanță sporită a sistemelor și o distribuire dinamică a resurselor, incluzând suportul *Direct Attached Storage* pentru memorare pe disc cu *cost minim* (lower-cost disk storage).

RDS (*Remote Desktop Services*) oferă clienților desktop-uri virtuale prin trei metode:

- *Mașini virtuale personale* (Personal VMs), prin care utilizatorul are acces la un *desktop virtual dedicat*, de înaltă performanță, asupra căruia are control administrativ complet.
- *Mașini virtuale partajate* (Pooled VMs), prin care se oferă clientului acces la desktopul virtual doar *la solicitarea acestuia*. Atunci când utilizatorul se deloghează, desktopul virtual este oferit altui client care îl solicită.
- *Desktop-uri bazate pe sesiune* (Session-based desktops), prin care clientul are acces la aplicații, date și desktop-uri partajate, care sunt centralizate pe server în Data Center.

Tabelul următor vă poate ajuta în alegerea *opțiunii* celei mai potrivite pentru *virtualizarea desktopurilor*:

	Desktopuri bazate pe sesiune	*Mașini virtuale partajate*	*Mașini virtuale personale*
Personalizare	++	++	+++
Compatibilitate	++	+++	+++
Management	+++	++	+
Cost minim	+++	++	+

Pentru detalii despre *Remote Desktop Services*, accesați linkul următor:
https://technet.microsoft.com/en-us/library/hh831447.aspx

Virtualizarea aplicațiilor

Microsoft oferă două soluții de virtualizare a aplicațiilor pe *Windows Server 2012, Windows Server 2012 R2* și *Windows Server 2016*: *RemoteApp* și *App-V*.

• *RemoteApp* este o virtualizare bazată pe *sesiune*. Aplicațiile rulează în *Data Center* și pot fi gestionate mai bine din punct de vedere al *securității* și *confidențialității* datelor.

Utilizatorii pot accesa de la distanță aplicațiile, fie prin intermediul unei *pagini web*, fie prin intermediul unui *client RDS (Remote Desktop Services*). Aceste aplicații pot rula alături de cele locale, în *ferestre redimensionabile* sau pe *monitoare multiple*, având *propriile iconuri* în meniul *Start* sau pe *taskbar*.

• *App-V* aparține de *MDOP* (Microsoft Desktop Optimizattion Pack). Aplicațiile sunt *împachetate* și transmise de pe server către client, *fără a fi necesară instalarea acestora*.

Aplicațiile virtualizate rulează pe echipamentele utilizatorilor în *medii virtuale autonome*, eliminându-se astfel *conflictele* dintre aplicații (puteți rula pe același computer versiuni diferite ale aceleiași aplicații sau puteți rula aplicații care, în mod normal, se exclud reciproc).

Administratorul *App-V* creează o secvență de aplicații pentru împachetarea acestora, pe care o memorează într-un fișier cu extensia *.appv* și o poate monitoriza în mod manual.

Împachetarea aplicațiilor virtuale se poate face prin *servere App-V* sau prin *Configuration Manager*.

Aplicația *App-V 5.0*, lansată odată cu *Windows 8*, oferă o *interfață complexă* de management a virtualizării aplicațiilor și include suport pentru *Windows PowerShell*, permițând crearea de scrípturi complexe pentru task-uri repetitive.

App-V 5.0 SP3 oferă îmbunătățiri ale *performanței* și *manevrabilității*, incluzând utilizarea *MSXML* (Microsoft XML Core Services) sau a *bibliotecilor Visual C++*.

App-V 5.1 conține suport pentru Windows 10 și vine cu foarte multe îmbunătățiri, care pot fi vizualizate accesând link-ul următor:

https://technet.microsoft.com/en-us/library/mt346500(v=vs.85).aspx #BKMK_Win10Support

Virtualizarea drive-urilor

Dacă datele de pe PC-ul dumneavoastră sunt extrem de importante şi nu vreţi să riscaţi pierderea acestora din cauza defectării hard disk-ului sau din cauza unor backup-uri eronate, puteţi alege soluţia *virtualizării drive*-urilor cu *Windows Storage Spaces*. Dacă datele nu ocupă un spaţiu prea mare, mai comodă este memorarea paralelă şi sincronă în cloud (*OneDrive*), pe serverele Microsoft, care asigură o protecţie maximă a datelor.

Virtualizarea drive-urilor a fost introdusă, în 2007, de *Windows Home Server* şi a fost preluată de *Windows 8* şi *Windows 10*. Avantajul principal constă în posibilitatea creării unui *drive virtual* de *orice capacitate*, indiferent de capacităţile hard drive-urilor fizice implicate în virtualizare.

Cea mai reuşită combinaţie este un *SSD* plus *două hard disk-uri* SATA identice. Pe *SSD* vor fi instalate *Windows şi aplicaţiile*, iar cele *două hard disk*-uri vor lucra în sistem *mirroring* (oglindire). Dacă un hard disk se defectează, el poate fi înlocuit cu altul. După un proces de *remirroring*, cele două hard disk-uri vor funcţiona normal.

Bineînţeles că, până veţi achiziţiona un nou hard disk, veţi putea lucra, în continuare, cu un singur hard disk, având grijă să salvaţi periodic datele importante pe un suport extern.

De remarcat este faptul că, dacă nu mai există spaţiu liber pe cele două drive-uri virtuale, Windows va solicita instalarea unui nou drive, care *nu trebuie să fie neapărat asemănător cu acestea* (poate fi intern, extern, IDE, SATA, SAS, eSATA sau pe USB). *Numele* şi *litera* asociate drive-ului virtual nu se vor schimba, dar *capacitatea* acestuia va creşte după adăugarea noului drive.

Observaţii:

- Toate datele de pe drive-ul adăugat *se vor pierde*!
- Drive-urile din *Storage Spaces* pot fi de *orice tip* (intern, extern, IDE, SATA, eSATA, SAS sau USB) şi *nu* necesită *hardware special* (ca în cazul RAID), totul fiind realizat de Windows 10.
- Drive-urile virtuale pot fi *partiţionate* şi *formatate* la fel ca orice hard disk fizic.
- Un drive virtual nu poate fi *defragmentat* sau verificat cu *Checkdisk*.
- Se pot crea şi utiliza *două mai multe drive-uri virtuale* (mai rar).
- *Mirroring*-ul din *Storage Space* este realizat prin *software*-ul inclus în Windows 10 şi nu trebuie confundat cu *RAID* (Redundant Array of Inexpensive Discs), care este realizat prin *hardware*.

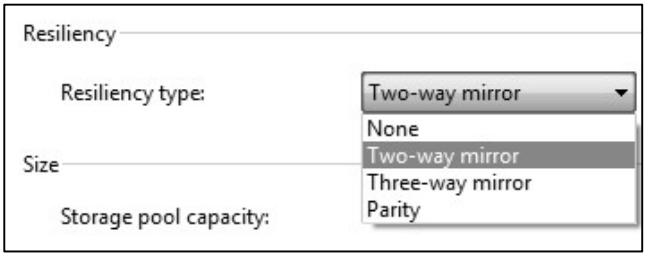
Există următoarele *posibilități* (resiliency) de a utiliza *Storage Space*:

• *None:* Datele nu sunt duplicate pe alt suport (există un singur hard disk).

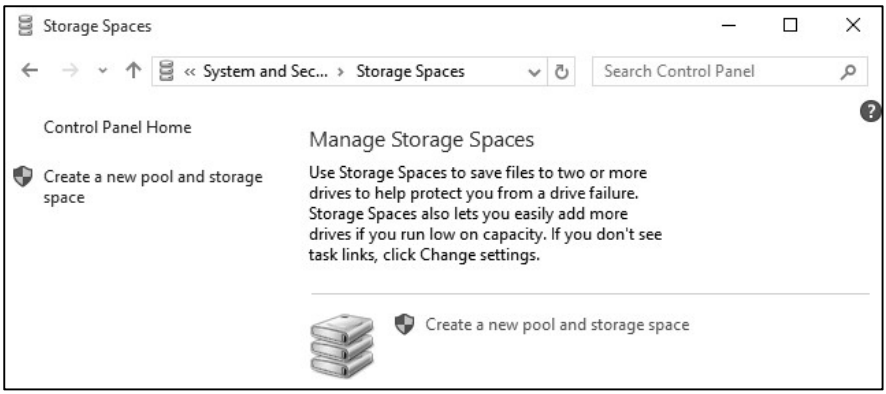
• *Two-way mirrored:* Mirroring-ul solicită cel puțin două hard diskuri, activitatea putând fi continuată dacă unul din acestea se defectează.

• *Three-way mirroring:* Mirroring-ul solicită cel puțin cinci hard diskuri.

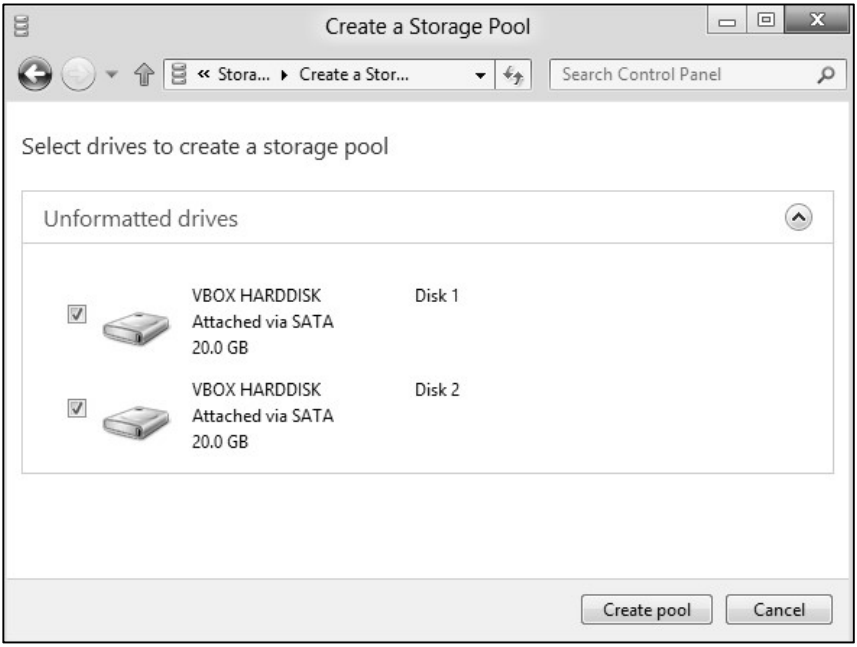
• *Parity:* Se utilizează cel puțin trei hard disk-uri, fără mirroring, dar se calculează în permanență o *sumă de verificare* (check sum) a datelor, permițând recuperarea automată a acestora în cazul în care apar *sectoare defecte* pe unul din hard disk-uri. Microsoft recomandă acest tip de *resiliency* pentru fișierele de *dimensiuni mari*, cum ar fi filmele, documentarele și secvențele video, sau pentru fișierele care nu sunt actualizate foarte des. Viteza de acces la drive-ul prin *Parity* este mai scăzută decât prin *Two-way mirrored* sau *Three-way mirroring*.



Pentru a *crea un drive virtual*, urmați calea *Start – Control Panel – System and Security – Storage Spaces – Create a new pool and storage space*.



Bifați cele două căsuțe din partea stângă a hard disk-urilor fizice care vor forma drive-ul virtual, apoi apăsați butonul *Create pool*.

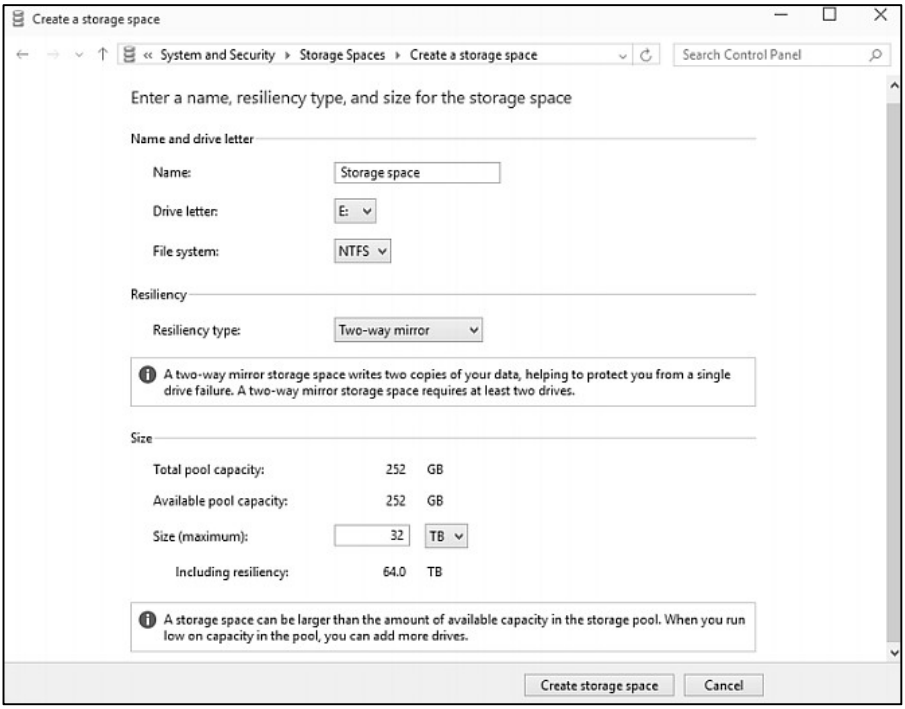


În fereastra *Create a storage space*, secțiunea *Name and drive letter*, tastați în căsuța *Name* numele drive-ului virtual (de exemplu VDISC), alegeți litera asociată drive-ului din lista derulantă *Drive letter* și selectați sistemul de fișiere din lista derulantă *File System* (aveți de ales între *NTFS* și *REFS* – este de preferat să-l alegeți pe primul).

În secțiunea *Resiliency* alegeți tipul de mirroring (*None, Two-way mirror, Three way mirror* sau *Parity*). În cazul nostru vom alege *Two-way mirror*.

În secțiunea *Size*, căsuța *Size (maximum)* tastați *capacitatea* drive-ului virtual în GB sau TB, care poate să fie mult mai mare decât a celor două hard disk-uri.

În final apăsați butonul *Create storage space* și așteptați formatarea drive-ului virtual. Veți fi redirecționați spre fereastra *Manage Storage Spaces* în care puteți *adăuga* alte drive-uri virtuale și puteți *redenumi* sau *șterge* drive-ul virtual.



Dacă veți deschide *File Explorer*, veți observa apariția drive-ului *VDISC*, cu *litera* asociată și cu *capacitatea* declarată anterior.

În momentul în care spațiul liber de pe drive-ul virtual este aproape epuizat, Windos 10 vă va avertiza printr-o *notificare*, solicitându-vă introducerea unui nou drive, de orice tip (intern, extern, IDE, SATA, eSATA, SAS sau USB).

UE-V, Folder Redirection și Work Folders

• *User Experience Virtualization* (UE-V) a fost lansată odată cu Windows 8 și permite administratorilor să centralizeze în *Data Center* aplicațiile și setările Windows, permițând utilizatorilor să acceseze aplicațiile virtuale din orice loc și de pe orice dispozitiv.

UE-V 2.1 oferă suport pentru aplicațiile *Windows Store* și pentru cele achiziționate intern prin *LOB* (Line-Of-Business).

Aplicația *sincronizează setările Windows* de pe stațiile de lucru (de exemplu desktop-urile, Microsoft Office 2010 și 2013, Internet Explorer 11 etc.).

• *Folder Redirection* completează UE-V 2.1 prin *centralizarea folderelor de date ale utilizatorilor* (documente, imagini, muzică etc.) în DataCenter, astfel încât acestea devin accesibile de pe orice computer la care utilizatorul se loghează utilizând credențialele sale.

• *Work Folders* a fost introdus odată cu Windows 8.1 și oferă îmbunătățiri semnificative față de *Folder Redirection*, cea mai importantă fiind *sincronizarea fișierelor pe dispozitive care nu aparțin unui domeniu.*

UE-V 2.1 SP1, pe lângă facilitățile oferite de versiunile anterioare, adaugă suport pentru *Windows 10* și alte îmbunătățiri substanțiale:

- ✓ Compatibilitate cu *Microsoft Azure*;
- ✓ Modificarea comportamentului în *sincronizarea setărilor*;
- ✓ Suport pentru *imprimante de rețea mobile* (roaming network printers);
- ✓ *Șabloane de setări* pentru Office 2013, cu suport pentru *semnături Outlook.*

Pentru detalii accesați următorul link:
https://technet.microsoft.com/en-us/library/mt427461(v=vs.85).aspx

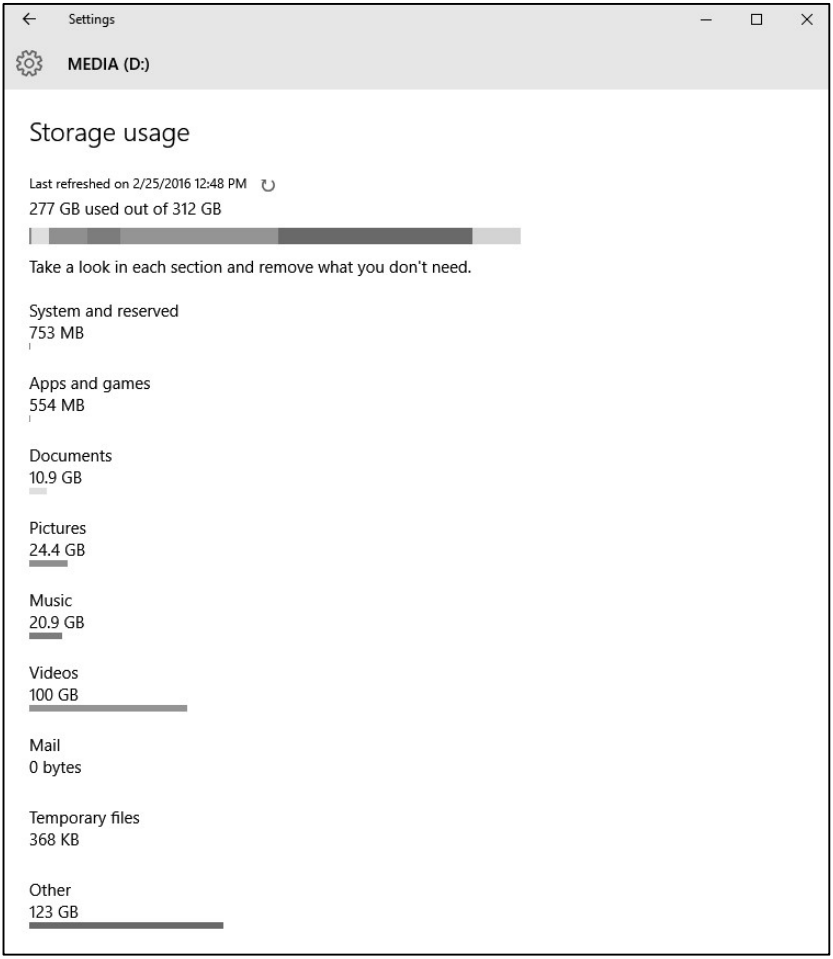
Configurarea și securizarea datelor

Managementul drive-urilor
OneDrive
OneDrive for Business
Autorizarea accesului la date
Convertirea drive-urilor și partițiilor la NTFS
Encrypted File System
BitLocker

Managementul drive-urilor

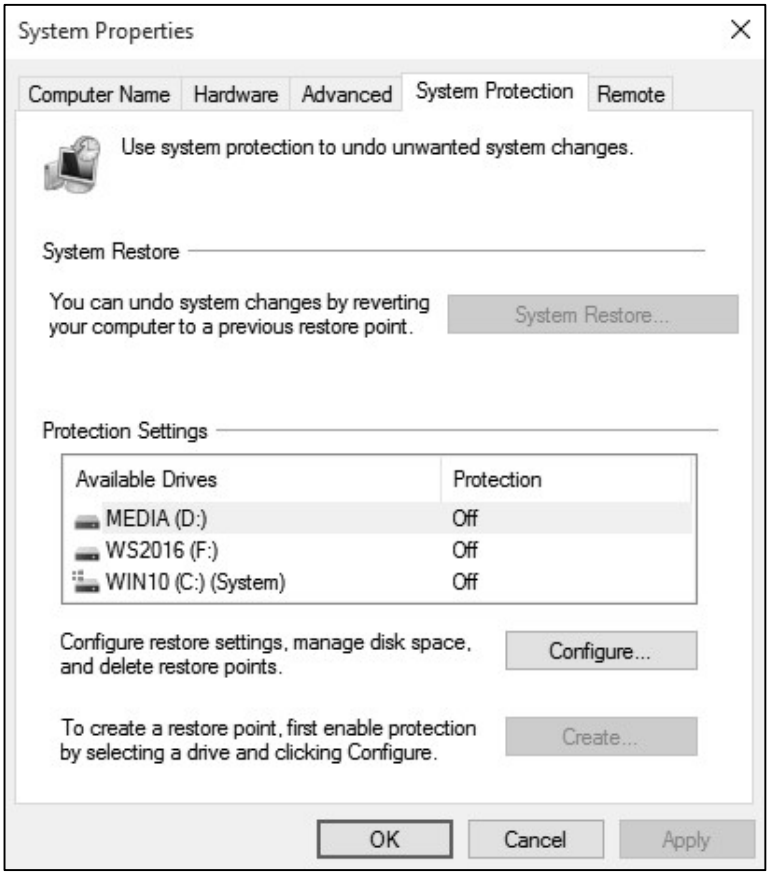
Pentru a vizualiza spațiul ocupat pe drive-urile sau pe partițiile unui PC, urmați calea *Start – Settings – System – Storage*.

Dacă veți da clic pe drive-ul sau pe partiția respectivă, veți obține o *afișare în culori* a modului în care este ocupat spațiul respectiv, iar dacă veți da clic, de exemplu pe *Music*, veți obține detalii despre muzica memorată pe drive.

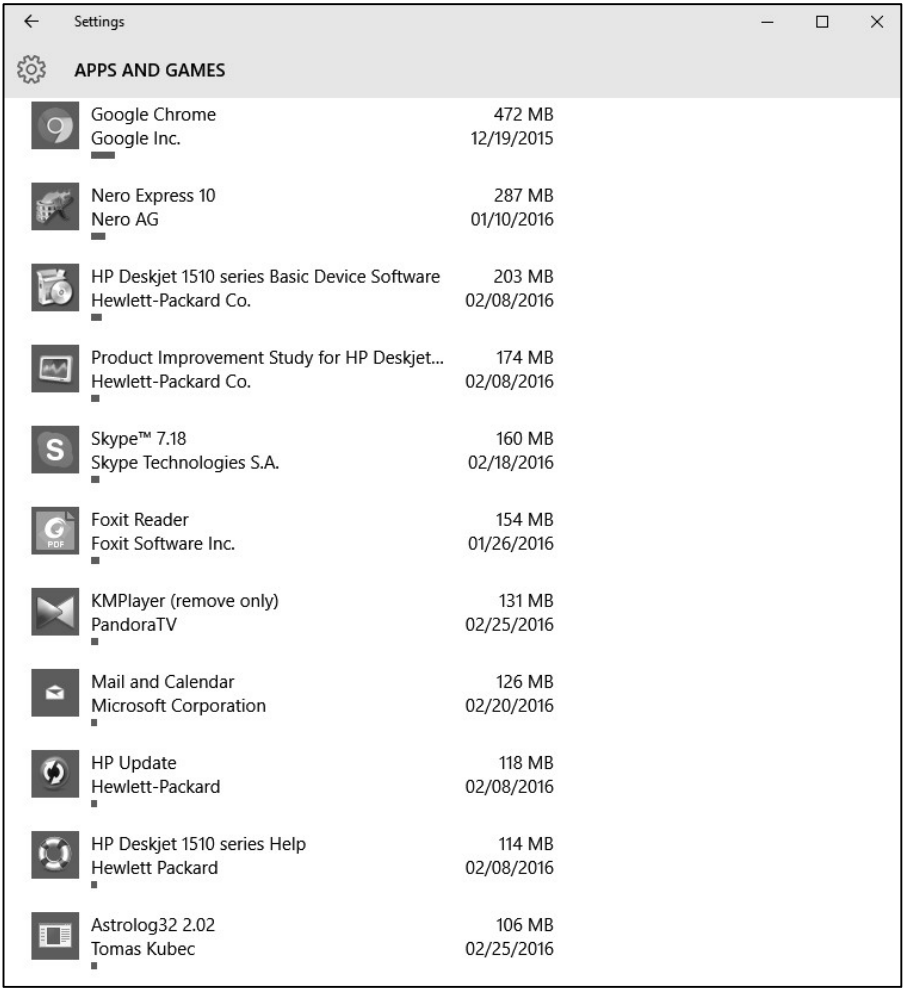


În fereastra *Storage*, secțiunea *Save Locations*, puteți seta *drive*-ul sau *partiția* pe care se vor salva ulterior *aplicațiile, documentele, imaginile, muzica* și *filmele.*

Dacă veți urma calea *Start – Settings – System – Storage* și veți da clic pe *This PC* în secțiunea *Storage*, apoi clic pe *System and Reserved* și veți apăsa butonul *Manage System Restore*, veți avea acces la fereastra *System Properties*, în care puteți fixa sau configura *puncte de restaurare* ale sistemului de operare (restore points).

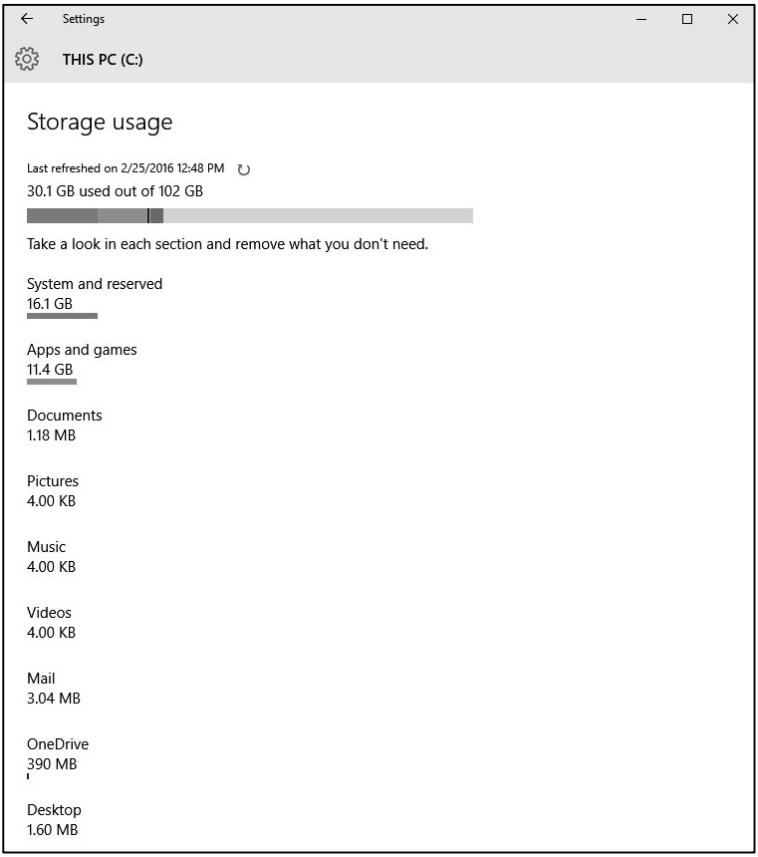


Dacă veți da clic pe *Apps and Games* în fereastra *This PC*, veți obține o listă completă a aplicațiilor instalate pe computerul respectiv.



Cu *clic* pe oricare din aplicații veți obține accesul la butonul *Uninstall*, cu care puteți dezinstala aplicația respectivă.

Procedând identic cu *System And Reserved* și *Apps and Games* din fereastra *This PC*, puteți vizualiza folderele în care se află *documentele, imaginile, muzica și filmele*, puteți administra *mailurile* din Outlook 2016 cu butonul *Manage Mail*, puteți sincroniza datele din *OneDrive* cu cele de pe PC prin butonul *Manage OneDrive*, reorganiza desktopul cu butonul *View desktop*, șterge fișierele temporare cu butonul *Delete Temporary Files*, vizualiza fișierele descărcate de pe Internet cu butonul *View downloads*, goli coșul de gunoi cu butonul *Empty recycle bin* sau șterge versiunea anterioară de Windows (*windows.old*) cu butonul *Delete Previous Versions*.



OneDrive

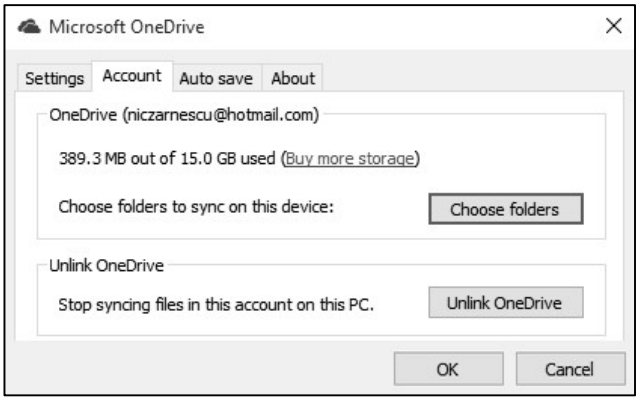
OneDrive este un fel de hard drive oferit în mod gratuit de Microsoft, pe care vă puteți păstra *copii ale fișierelor personale* (muzică, imagini, documente etc.) și pe care le puteți accesa de pe orice dispozitiv conectat la Internet (tabletă, smartphone, 2-in-one, laptop-uri, all-in-one sau PC), indiferent de sistemul de operare utilizat de acesta (Windows, iOS sau Android).

Cunoscut anterior ca *Live FolderShare, Live Mesh, Live Sync* sau *SkyDrive, OneDrive* are un spațiu de stocare de 15GB.

Pentru a afla și alte oferte de stocare pe *OneDrive*, accesați site-ul *https://onedrive.live.com* și dați clic pe opțiunea *Upgrade* din stânga-jos.

Microsoft a anunțat în februarie 2016 că va reduce spațiile de stocare din cauza suprasolicitării serverelor (vezi *https://onedrive.live.com/about/en-us/plans*).

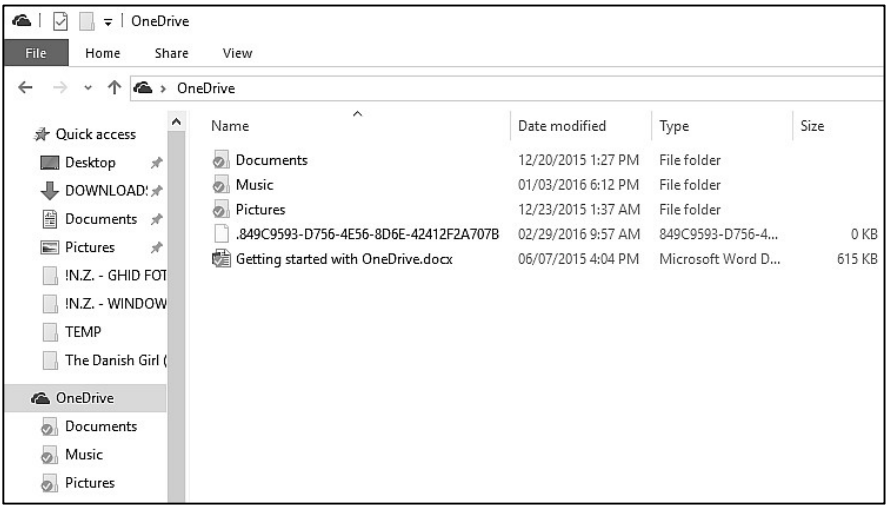
Pentru a afla *spațiul real de stocare* de care dispuneți, dați clic pe simbolul ^ aflat în dreapta taskbar-ului, *clic drept* pe simbolul nor și alegeți *Settings*, apoi apăsați tabul *Account*.



Dacă apăsați butonul *Choose folders*, apare o listă a folderelor de pe *OneDrive* pe care le puteți sincroniza cu foldere de pe PC (*Sync your OneDrive files to this PC*). În acest fel, orice modificare a conținutului folderelor locale se va reflecta automat în folderele de pe *OneDrive*. Fereastra *Sync your OneDrive files to this PC* se poate obține și urmând calea *Start – Settings – System – Storage – This PC – OneDrive – Manage OneDrive*. Folderele și fișierele sincronizate au o bifă verde.

Pentru accesarea lui *OneDrive* pe PC este suficient să aveți un *cont Microsoft* și să vă *logați* cu acesta sau să accesați site-ul *https://onedrive.live.com* de pe alt dispozitiv conectat la Internet, cu același cont Microsoft.

În Windows 10, pentru a accesa fișierele din *OneDrive*, deschideți *File Explorer* și expandați *OneDrive* din panoul de navigare aflat în partea din stânga.



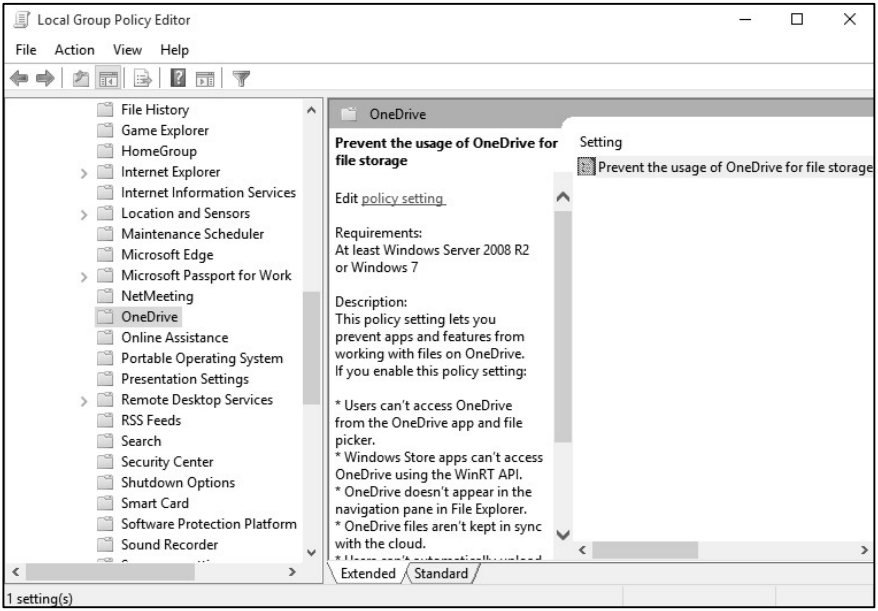
Documentele, muzica și imaginile pot fi stocate în *OneDrive* prin *Copy* și *Paste*, prin *drag and drop* sau prin *salvare* din orice aplicație.

Partajarea folderelor și fișierelor cu prietenii se poate face cu opțiunea *Share* a meniului superior al lui *File Explorer* sau cu *clic drept* pe folderul sau fișierul respectiv, apoi alegând *Share*. În partea din dreapta-jos a folderului partajat, apare un simbol cu două persoane.

Setări amănunțite pentru *OneDrive* se pot face cu clic pe simbolul ^ aflat în dreapta taskbar-ului, *clic drept* pe simbolul nor și alegeți *Settings*, apoi apăsați taburile *Settings* și *Auto Save*. Apăsând tabul *About*, puteți obține *informații* suplimentare despre OneDrive.

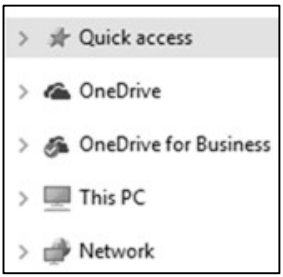
Dacă doriți să asociați *OneDrive* unui alt cont Microsoft, în tabul *Settings* apăsați butonul *Unlink OneDrive* (vezi pagina următoare).

Se poate stabili și *o politică de grup* (group policy) pentru utilizarea lui OneDrive tastând *gpedit.msc* în căsuța de căutare pentru Cortana, *gpedit.msc (Microsoft Common Console Document*). În panoul din stânga extindeți arborele *Computer Configuration – Administrative Templates – Windows Components – OneDrive*. Dați clic pe opțiunea din dreapta *Prevent the usage of OneDrive for file storage* și clic pe *Enable* în fereastra care apare. OneDrive va deveni indisponibil.



OneDrive for Business

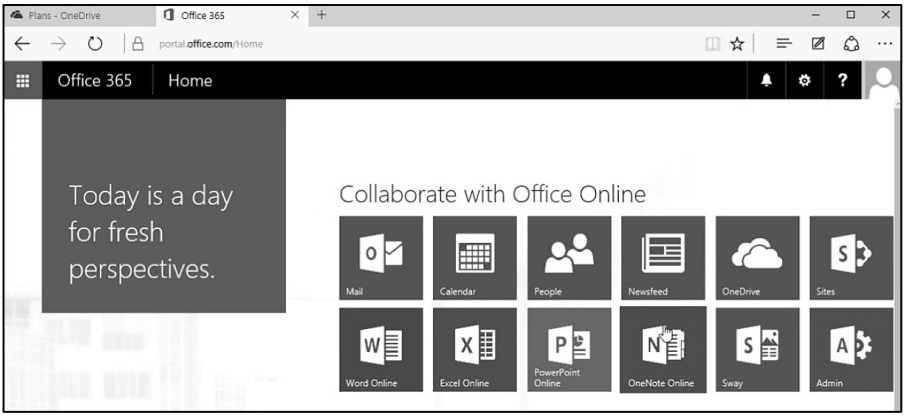
OneDrive for Business oferă fiecărui utilizator, pentru 6,99$ pe lună, un spațiu de 1TB, împreună cu posibilitatea utilizării pachetului *Office 365*. Dacă sunt 5 utilizatori, tariful lunar este de 9,99$ (vezi *onedrive.live.com/about/en-us/plans*).



OneDrive for Business este mult mai complex decât *OneDrive* și oferă mai multe facilități. Acesta nu este inclus în pachetul lui Windows 10 și este necesară instalarea aplicației *OneDrive for Business Sync App* și a uneia din versiunile de *Microsoft Office Plus 2013* sau *2016*, apoi intalarea lui *Office 365 Enterprise E3, Office 365 Midsize Business* și *Office 365 Small Business Premium*.

Mai simplă este descărcarea update-ului *KB2903984* și instalarea acestuia.

OneDrive for Business apare în *File Explorer* imediat sub *OneDrive*. Modul de lucru cu fișierele și folderele din *OneDrive for Business* este același ca cel cel din *OneDrive*, dar accesul online de pe alt dispozitiv se face cu linkul *http://portal.office.com,* apoi cu clic pe tile-ul *OneDrive*.



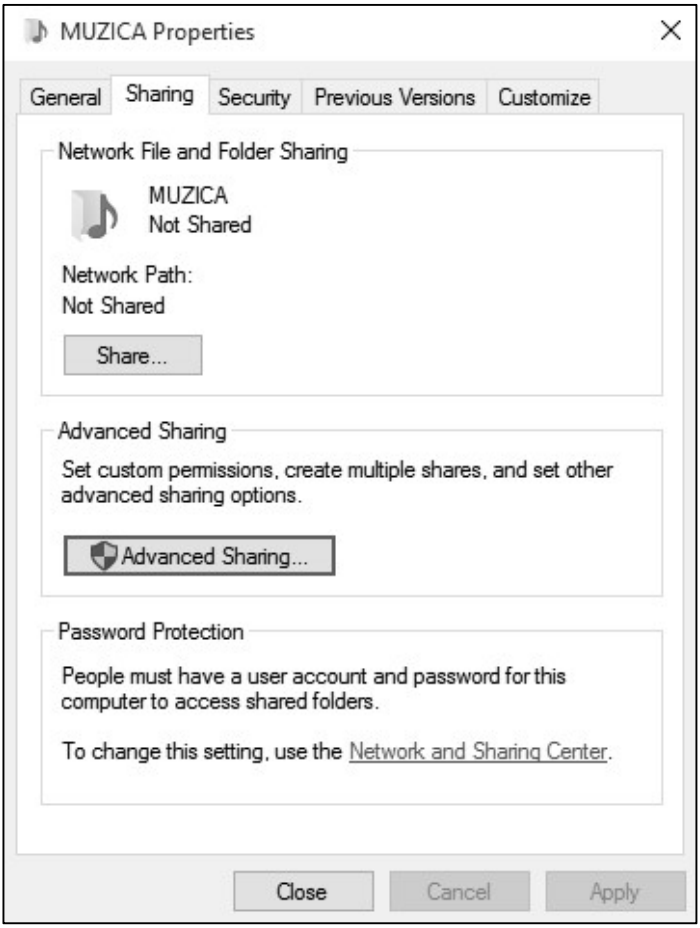
Mai există încă două variante de utilizare a lui *OneDrive for Business:*

- *OneDrive for Business with Office Online* (25GB sau mai mult);
- *OneDrive for Business with Internal SharePoint Farm* (asigură o securitate sporită a datelor în cloud, prin criptarea acestora, alături de alte facilități).

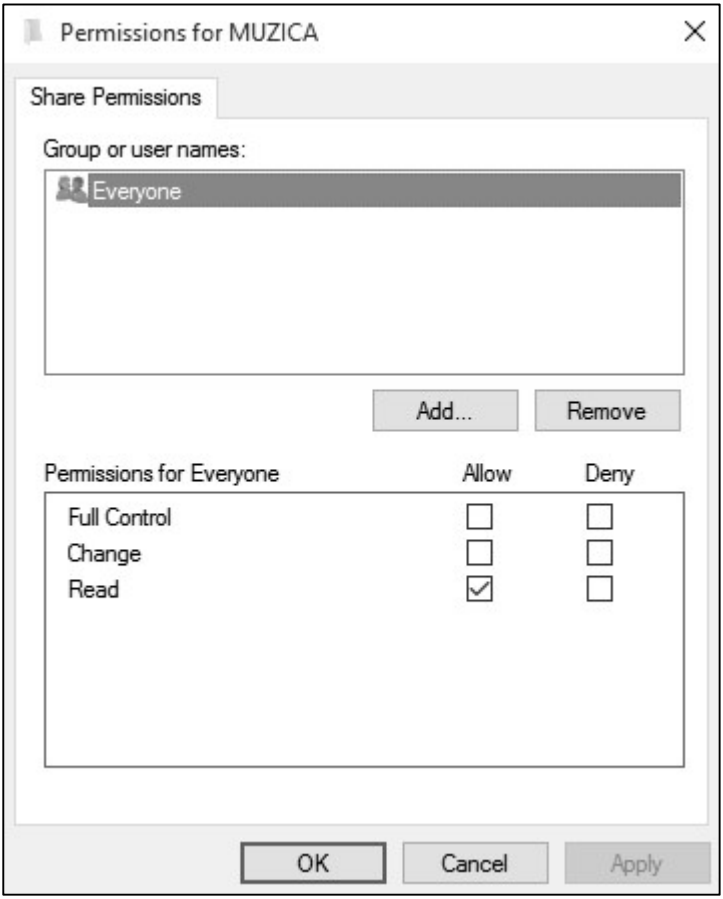
Autorizarea accesului la date

Permisiuni simple de partajare

Puteți *partaja* anumite foldere cu prietenii dintr-o rețea locală sau cu cei de pe Internet. Pentru a partaja un *folder* (de exemplu MUZICA), dați *clic drept* pe folderul respectiv și alegeți *Properties* din meniul contextual, apoi apăsați tabul *Sharing* și butonul *Advanced Sharing*.



În fereastra *Advanced Sharing* care apare, bifați *Share this folder*. Pentru a vedea permisiunile asociate folderului, apăsați butonul *Permissions*.



Implicit este bifată căsuța *Read*, deci prietenii dumneavoastră vor putea doar deschide fișierele respective (asculta muzica). Dacă bifați și *Change* prietenii vor putea modifica fișierele (denumire sau conținut), dar nu le vor putea șterge. Pentru oferi acces complet la fișierele folderului, bifați *Full Control*.

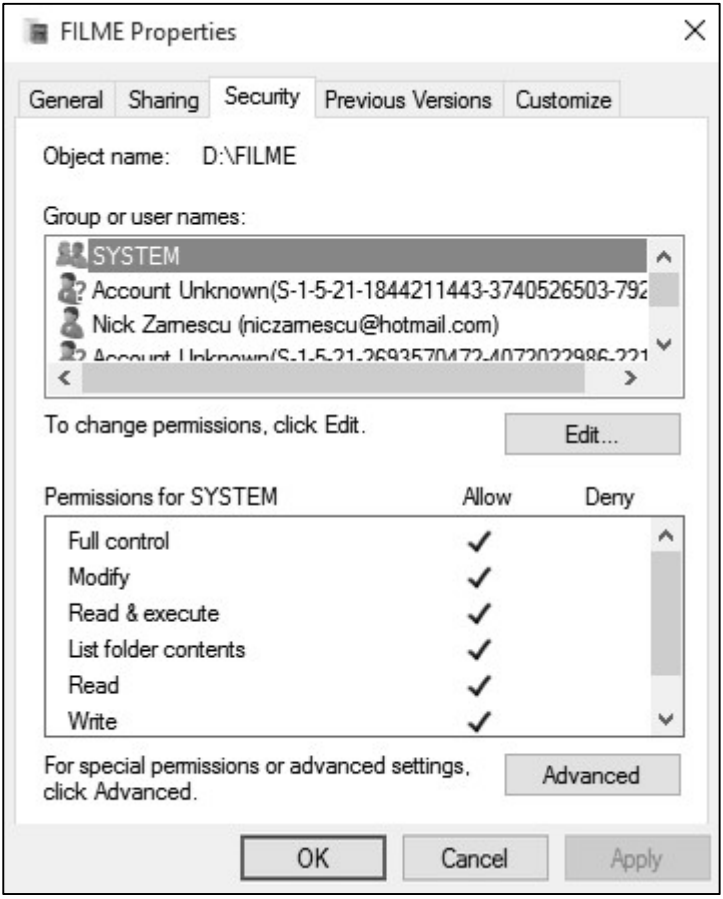
Accesul poate fi interzis prin bifarea căsuțelor din coloana *Deny*.

Permisiuni NTFS de partajare

Altă modalitate de a partaja folderele este aceea a permisiunilor NTFS, accesibile doar în cazul în care hard diskul a fost formatat în NTFS.

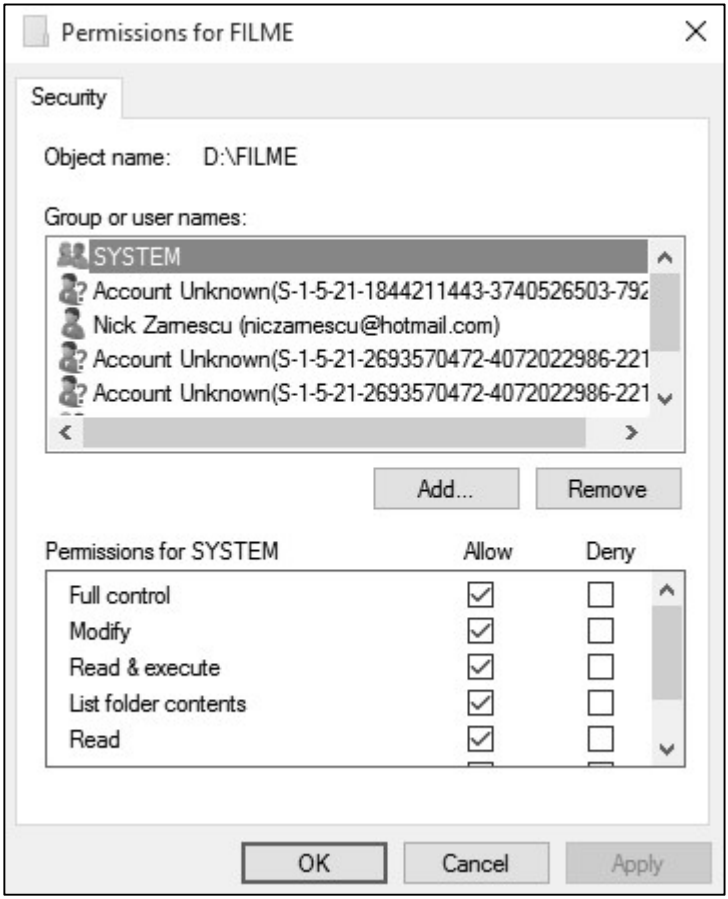
Pentru a partaja un folder prin permisiuni NTFS (de exemplu FILME), dați *clic drept* pe folder, alegeți *Properties* din meniul contextual și apăsați tabul *Security*.

Tipurile de permisiuni NTFS sunt următoarele: *Full Control, Modify, Read & Execute, List Folder Contents, Read, Write* și *Special Permisions*. Pentru setări avansate, apăsați butonul *Advanced*.



În secțiunea *Group or user names* sunt afișate grupurile și utilizatorii individuali care vor avea acces la folderul respectiv.

Pentru a modifica permisiunile, apăsați butonul *Edit*.



În coloana *Allow* autorizați un anumit tip de acces, iar în coloana *Deny* interziceți accesul.

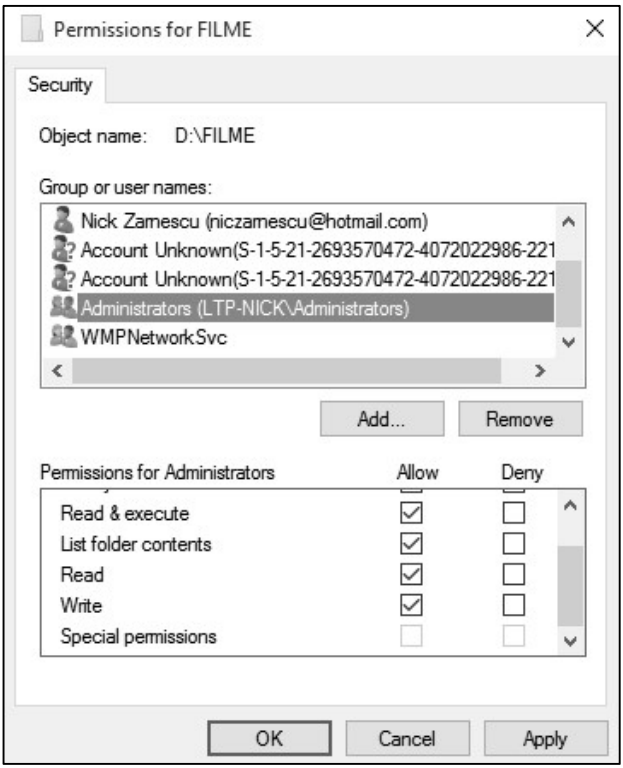
Permisiunea *Full Control* este asemănătoare cu cea din permisiunile simple de partajare. *Modify* permite citirea, modificarea și ștergerea fișierului din folder.

Selectarea opțiunii *Modify* are ca efect bifarea automată a opțiunilor următoare (*Read & Execute, List Folder Contents, Read, Write*).

Read & Execute permite doar citirea (dacă este vorba de un document) și eventual lansarea în execuție (dacă este vorba de o aplicație). Selectarea acestei opțiuni are ca efect bifarea automată a opțiunilor *List Folder Contents* și *Read*.

List Folder Contents permite doar afișarea conținutului folderului și se aplică doar folderelor, nu și fișierelor individuale.

Read permite doar citirea documentelor, iar *Write* permite atât citirea, cât și crearea sau modificarea conținutului documentelor, ștergerea sau sincronizarea acestora. *Special Permitions* autorizează accesul la date în alt mod decât cele amintite anterior.



Convertirea drive-urilor și partițiilor la NTFS

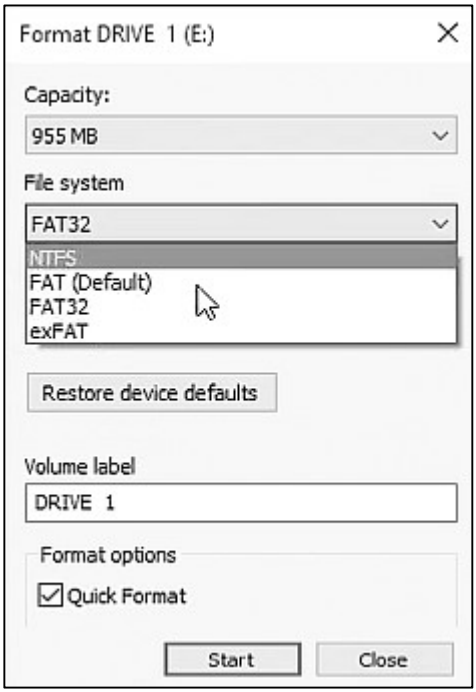
Există trei sisteme de formatare a drive-urilor și partițiilor:

• FAT – utilizat de Windows 95, Windows 98 și Windows Millenium;

• FAT32 – utilizat în versiunile anterioare de Windows (prin convertirea la NTFS, datele de pe drive sau partiție nu sunt afectate);

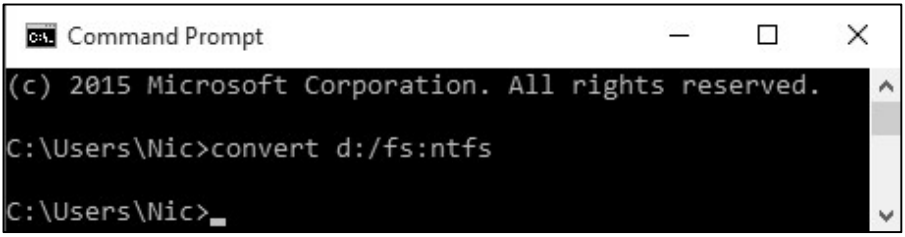
• NTFS – asigură o performanță mai bună și o securitate sporită (recuperarea automată a datelor în cazul apariției erorilor pe drive, crearea partițiilor mai mari de 32GB, stocarea fișierelor mai mari de 4GB și criptarea datelor).

Pentru a *formata* un drive în NTFS, dați *clic drept* pe drive-ul respectiv și alegeți *Format*. Selectați *NTFS* din lista derulantă a secțiunii *File System*, bifați *Quick Format* pentru o formatare rapidă, apoi apăsați butoanele *Start* și *OK*.



Pentru a converti un drive sau o partiție de la *FAT32* la *NTFS*, dați *clic drept* pe butonul *Start* și alegeți *Command Prompt* din meniul contextual.

Tastați la *prompter* următoarea comandă: ...>*convert d:/fs:ntfs*, apoi apăsați tasta *Enter*.



Conversia poate *eșua* dacă driver-ul sau partiția sunt aproape pline, de aceea *ștergeți* datele neimportante sau efectuați un *backup* înainte de conversie.

Conversia la NTFS este ireversibilă. Dacă vreți să reveniți la FAT32, faceți un backup al datelor, apoi reformatați partiția cu FAT32.

Enterprise Data Protection (EDP)

Utilizarea pe acelaşi echipament atât a *datelor personale*, cât şi a *datelor instituției*, sporește riscul *breşelor de securitate* şi al *atacurilor malware* din exterior, în rețelele nesecurizate.

Prin *EDP*, utilizatorul poate accesa în siguranță atât *datele personale*, cât şi *datele instituției* (de exemplu mailurile). Dacă angajatul îşi schimbă locul de muncă, datele instituție vor fi *şterse* în mod automat.

Smartphone-urile de generație mai nouă conțin *containere* pentru criptarea automată a datelor care aparțin instituției.

Pentru a configura EDP, trebuie să vă stabliți mai întâi o *listă a resurselor* instituției, care vor fi accesate (adrese IP, domenii, email-uri). Acestea vor fi recunoscute implicit ca *date importante aparținând instituției*, vor fi *criptate* în mod automat şi vor fi memorate în *containere virtuale*.

Puteți stabili şi o *listă a aplicațiilor* autorizate care vor utiliza EDP, cum ar fi *Outlook, SharePoint* sau alte aplicații pe care le utilizați *acasă*.

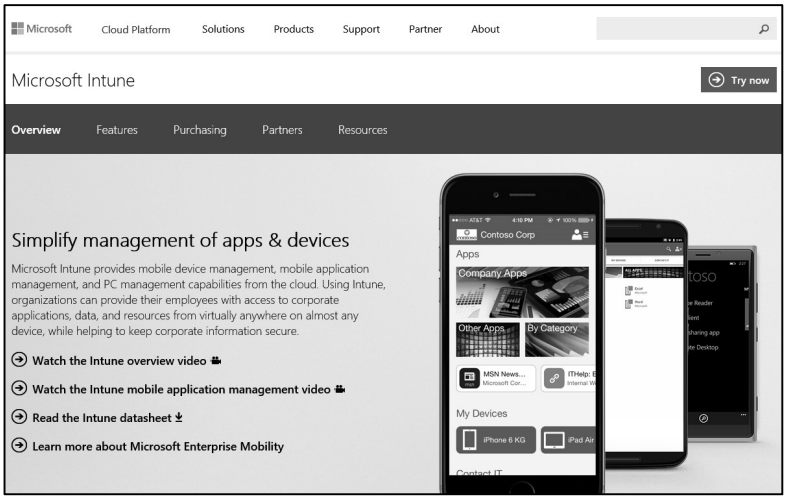
EDP oferă patru nivele de protecție: *Block* (blocarea funcțiilor Copy şi Paste), *Override* (permite Paste, dar avertizează utilizatorul că va păstra blocată o copie a documentului), *Audit* (management real) şi *Off*. Nu este recomandabil să utilizați *Off*, dacă anterior ați utilizat *Block, Override* sau *Audit*, deoarece toate politicile de securitate ale datelor vor fi şterse şi va trebui să le recreați.

EDP este inclus în Windows 10, edițiile *Pro, Enterprise* şi *Education*, iar manangementul acestuia se face cu *Windows Server 2012 Configuration Manager* de pe serverul din rețea, cu aplicația de management *achiziționată de instituția respectivă* sau cu aplicația *Microsoft Intune Mobile Application Management* (MAM), despre care puteți găsi detalii importante la următorul link: *https://www.microsoft.com/en-us/server-cloud/products/microsoft-intune*.

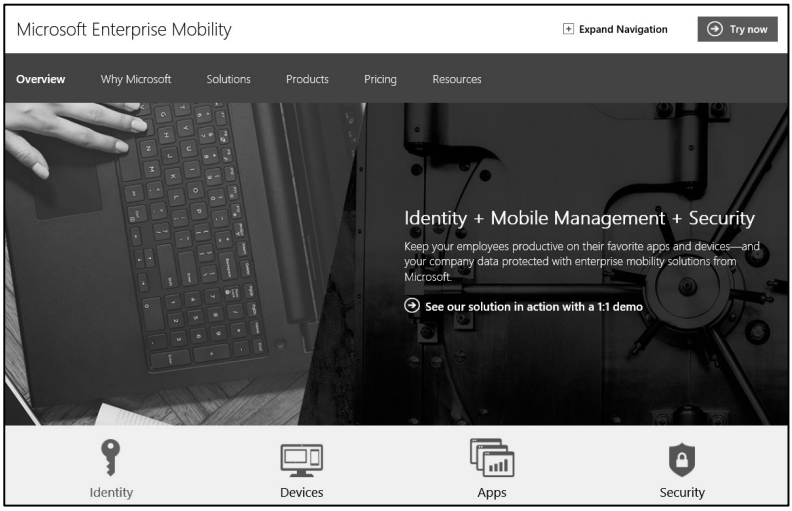
Aplicația *Microsoft Intune* recunoaşte *Microsoft Office, Active Directory, Azure Active Directory* şi *System Center* şi veți putea accesa rețeaua instituției indiferent de locul în care vă aflați, prin intermediul lui *System Center Configuration Manager* sau prin *Intune Management Console*.

Microsoft Intune este inclus în *Enterprise Mobility Suite (EMS)* şi oferă *protecția identității*, un *management hybrid al identității* şi *managementul de pe dispozitive mobile* (tabletă sau smartphone).

Protecția cu *Intune* poate fi utilizată şi la *nivele superioare* (Azure Rights Management). *Intune* lucrează în mod direct cu *Office365*, pentru a proteja datele care aparțin instituției.



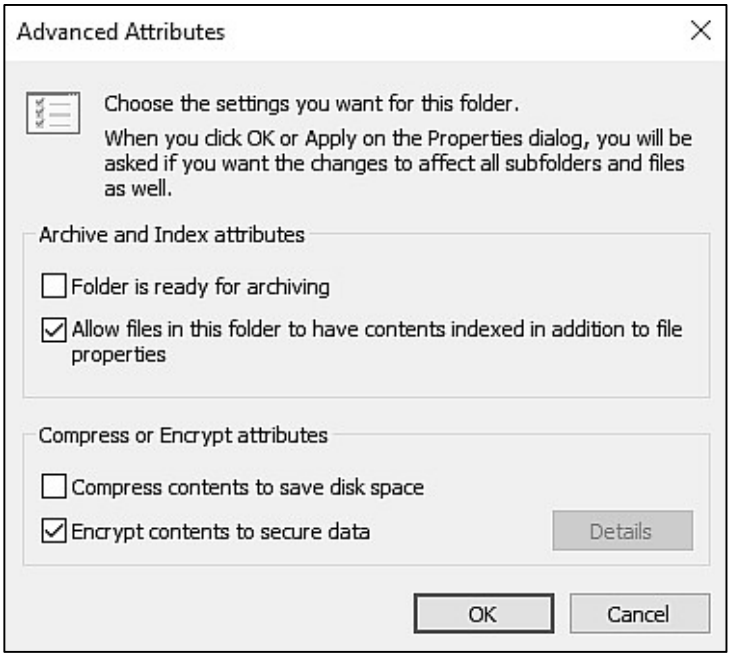
Detalii despre serviciile *Microsoft Enterprise Mobility* puteți găsi și pe site-ul *https://www.microsoft.com/en-us/server-cloud/enterprise-mobility*.



Encrypted File System (EFS)

Prin *EFS* se asigură o criptare de înaltă securitate a volumelor *NTFS*. Criptarea sau decriptarea utilizează o *cheie privată* (Private Key), memorată în profilul utilizatorului, sau o *cheie de recuperare* (Master Recovery Key), memorată de agentul de recuperare.

Pentru a *cripta un fold*er cu EFS (de exemplu DOC), daţi *clic drept* pe folder şi selectaţi *Properties*. În fereastra *DOC Properties* apăsaţi butonul *Advanced*, apoi bifaţi *Encrypt contents secure data* şi apăsaţi *OK*, iar în final apăsaţi butonul Apply, în fereastra iniţială.



Veţi fi întrebat dacă se va face doar criptarea *folderului* respectiv sau vor fi criptate, de asemenea, *subfolderele* şi *fişierele*. Apăsaţi unul din cele două *butoane radio* care apar, apoi apăsaţi butonul *OK*.

În final, apăsaţi butonul *OK* în fereastra *DOC Properties* şi aşteptaţi terminarea criptării folderului.

Dacă doriți să criptați doar un fișier, utilizați aceeași procedură ca la criptarea unui folder.

Pentru a decripta folderul sau fișierul criptate anterior, dați *clic drept* pe folder și selectați *Properties*. În fereastra *Properties* apăsați butonul *Advanced*, apoi debifați *Encrypt contents secure data* și apăsați *OK*, iar în final apăsați butonul *Apply*, în fereastra inițială.

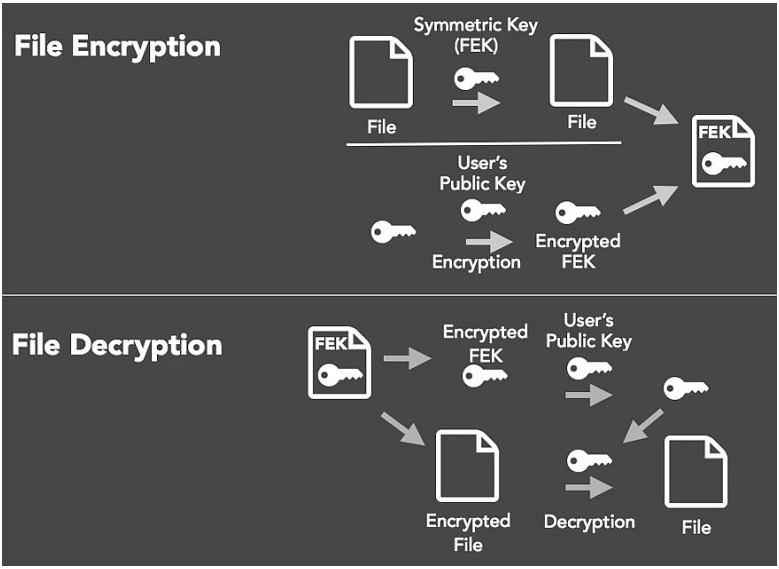
Veți fi întrebat dacă se va face doar decriptarea *folderului* respectiv sau vor fi decriptate, de asemenea, *subfolderele* și *fișierele*. Apăsați unul din cele două *butoane radio* care apar, apoi apăsați butonul *OK*.

În final, apăsați butonul *OK* în fereastra *Properties* și așteptați decriptarea.

Copierea unui fișier într-un folder criptat are ca rezultat criptarea automată a acestuia. Și reciproca este adevărată: dacă copiați într-un folder necriptat un fișier criptat, acesta va fi decriptat în mod automat.

Iată câteva recomandări generale privind utilizarea EFS:

- Exportați *cheile private* și *certificatele* pe un drive extern (stick USB);
- Ca administrator, puteți cripta toate folderele *My Documents* din rețea;
- Întotdeauna criptați *foldere* și nu fișiere individuale.



Imagine publicată de Microsoft

BitLocker

BitLocker a fost introdus începând cu *Windows Vista Ultimate*, fiind apoi perfecţionat pe sistemele cu *Windows 7 Ultimate, Windows 8.x Pro* şi *Enterprise*, *Windows 10 Pro*, *Enterprise*, *Education* şi *IoT Core*.

Bitlocker permite atât *criptarea* drive-urilor *interne*, cât şi a celor *externe*, conectate pe USB şi este mai rapid decât în Windows 7 sau versiuni anterioare.

Pentru a putea deveni funcţional, BitLocker necesită *TPM 2.0* şi existenţa a cel puţin *două partiţii* pe drive-ul care trebuie criptat. Se pot cripta doar *porţiunea din partiţie care conţine date* sau *întreaga partiţie*, dar în acest al doilea caz timpul de criptare va fi mai lung.

Bitlocker este funcţional atât pe sistemele pe 32 biţi, cât şi pe cele pe 64biţi, dacă este prezent *TPM* ce suportă *Connected Standby*, introdus de Windows 8 sau *InstantGo* introdus de Windows 8.1). Prin aceste facilităţi se asigură conectivitate la Internet în modul *standby*, cu consum minim de resurse, descărcarea anumitor fişiere sau recepţionarea email-urilor fiind active în tot acest timp.

Şi *Azure Active Directory* poate beneficia de criptarea prin BitLocker, *cheia de criptare* fiind memorată într-un loc sigur de pe serverul AD.

Accesul direct la memorie (DMA – Direct Memory Access) poate fi *criptat* cu BitLocker, controlând-se *porturile de acces* cu ajutorul unor *chei criptate*.

Se poate cripta cu BitLocker *o întreagă reţea de calculatoare*, accesul la date fiind securizat foarte strict.

Spre deosebire de vechiul sistem de criptare a datelor de pe hard disk (EFS – *Encrypting File System*), care acţiona după încărcarea sistemului de operare, *BitLocker* acţionează înaintea încărcării acestuia, criptând *partiţia activă*.

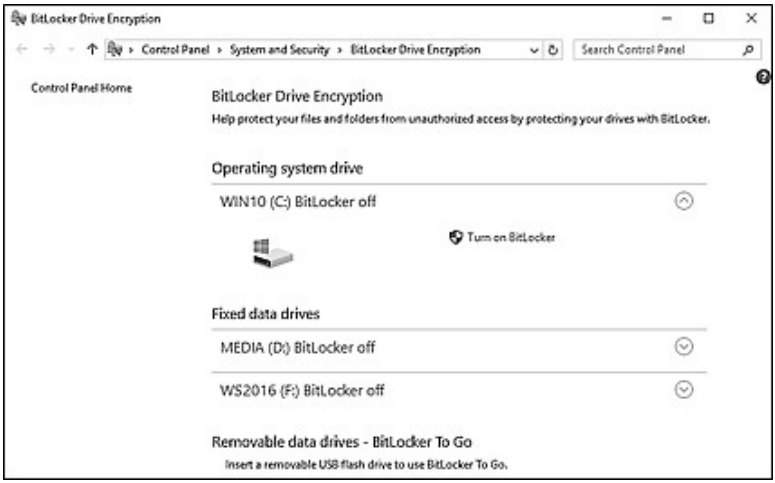
Dacă un echipament (PC, laptop, tabletă, smartphone) este furat, *datele de pe hard disk nu mai pot fi accesate prin nicio metodă*.

Există şi varianta *BitLocker To Go*, care este similar cu BitLocker-ul usual, doar că lucrează cu *stick-uri USB*. Dacă pierdeţi stickul, datele nu vor putea fi accesate.

Trebuie precizat că BitLocker este funcţional doar la *Windows 10 Pro* sau *Enterprise*, aşa că, dacă aveţi instalat *Windows 10 Home* şi vreţi să beneficiaţi de BitLocker, trebuie să faceţi *upgrade* la Windows 10 Pro.

Pentru a *instala* BitLocker, trebuie să vă alegeţi o perioadă de inactivitate mai lungă, deoarece operaţiunea este *mare consumatoare de timp*.

Tastaţi *bitlocker* în căsuţa de căutare pentru Cortana, apoi selectaţi *Manage BitLocker*. Va apărea fereastra din pagina următoare:



Dacă doriți să criptați un anumit *drive* (în cazul nostru WIN10), selectați opțiunea *Turn On Bitlocker* aflată în dreapta driverului respectiv, apoi răspundeți cu *Yes* la mesajul care apare.

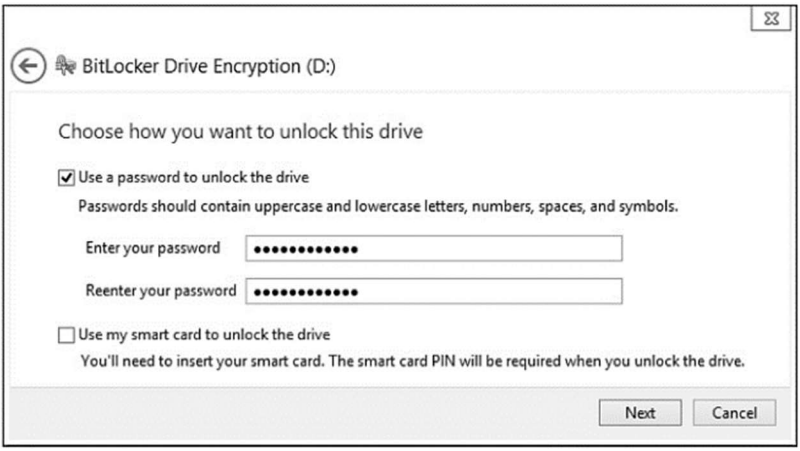
Dacă pe computer nu există *TPM* (Trusted Platform Module), atunci va apărea mesajul *Your administrator must see the 'Allow BitLocker without a compatible TPM'*. Acesta trebuie să apeleze *Local Group Policy Editor* tastând *gpedit.msc* în căsuța de căutare pentru Cortana și să permită *rularea lui BitLocker fără TPM*.

După ce alegeți *Next* de două ori, va apărea o fereastră în care vi se va solicita modul în care veți face *deblocarea* drive-ului criptat cu Bitlocker: printr-o *parolă complexă* sau prin *smartcard cu PIN*.

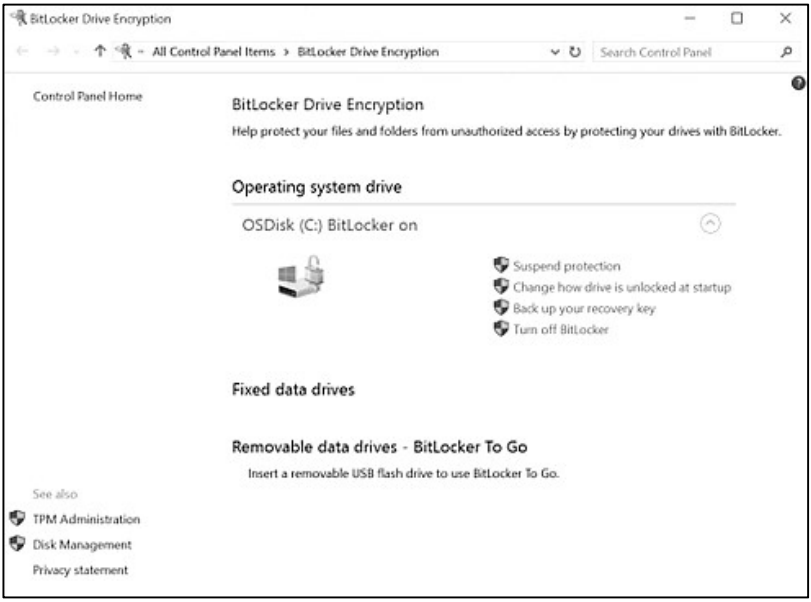
Introduceți parolele și dați clic pe Next, alegeți *Require a Startup Key at Every Startup*, apoi *Save the Recovery Key to a USB Flash Drive* și urmați indicațiile care apar pe display.

În afară de *USB Flash Drive*, puteți alege să salvați cheia de recuperare (recovery key) în *contul Microsoft*, într-un *fișier* sau să o *printați*. Este recomandabil să utilizați, pentru securitate sporită, cel puțin *două metode* (de exemplu stick USB și printare).

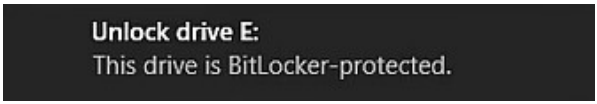
Bifați căsuța *Run Bitlocker System Check*, apoi dați click pe *Continue*. Vi se va solicita aprobarea pentru *reboot* și procesul de criptare va începe. Durata este de câteva *minute* pe un stick până la câteva *ore* pe un drive.



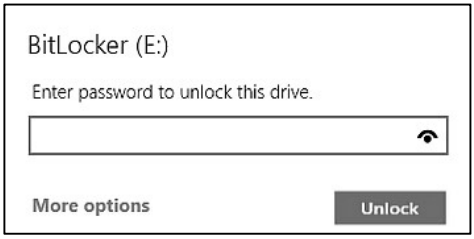
În fereastra de confirmare a criptării (*BitLocker Drive Encription*) va apărea opţiunea *Manage BitLocker.* Un drive criptat cu *BitLocker* va avea următoarele setări, care pot diferi în funcţie de metodele de criptare utilizate:



Când veți accesa un drive criptat cu BitLocker, veți observa o notificare în partea din dreapta-jos a display-ului:



Dați clic pe această notificare și vi se va solicita parola pentru deblocare:



Atunci când *BitLocker Drive Encryption* este activat, un administrator de rețea poate utiliza *Group Policy* pentru a stabili dacă se criptează doar spațiul *utilizat* de pe hard disk (Used Disk Space Only) sau *întregul spațiu* (Full Disk Encryption).

Deschideți *Local Group Policy Editor* și expandați arborele *\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption*, care are următoarele setări:

- *Fixed Data Drives* – setează tipul de criptare pe drive-urile cu date;
- *Operating System Drives* – setează tipul de criptare pe drive-urile care conțin sisteme de operare;
- *Removable Data Drives* – setează tipul de criptare pe drive-urile mobile;

Bitlocker suportă și *criptarea hardware* (Encrypted Hard Drive), utilizând un *controler* care accelerează procesul respectiv (storage controller) și care este detectat în mod automat de către Windows 10. Managementul hard disk-urilor criptate se face cu aplicația *BitLocker Control Panel*.

În rețelele mari, administratorii pot cripta doar *datele importante* ale instituției, lăsând necriptate datele personale ale utilizatorilor. Dacă angajatul își încheie contractul cu instituția respectivă, datele criptate (de exemplu mail-urile) sunt șterse în mod automat (wiped) sau devin inacesibile, prin acționarea automată a clientului *Exchange ActiveSync* (cu sau fără protocol OMA-DM).

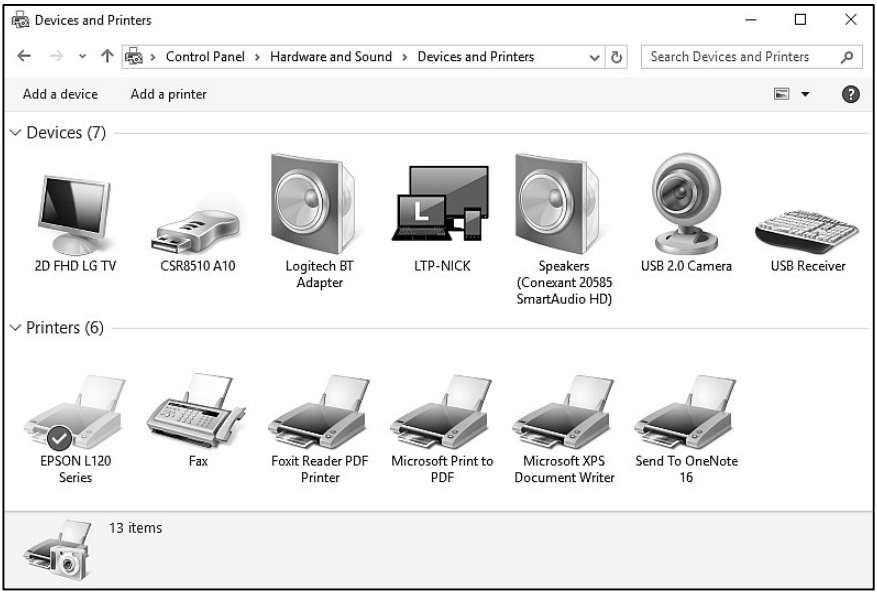
Partajarea resurselor

Partajarea imprimantelor
Partajarea cu HomeGroups
Partajarea folderelor și fișierelor

Partajarea imprimantelor

Dacă o imprimantă, indiferent de tip, este conectată prin *cablu USB* şi are instalat *driverul* corespunzător pe un computer aflat într-o reţea, atunci aceasta poate fi partajată de către membrii reţelei. Computerul poate rula sub Windows XP, Vista, 7, 8 sau 10. Imprimanta poate fi conectată şi *wireless* la un *access point*.

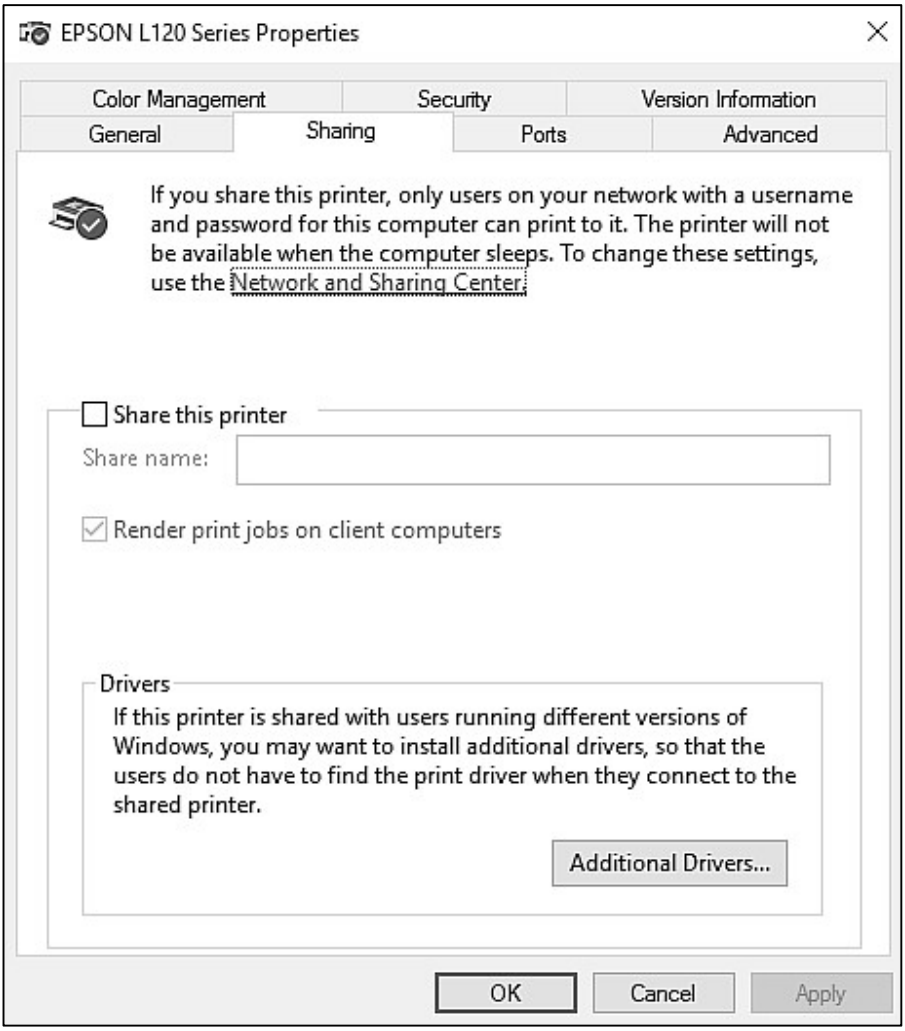
Primul pas este *localizarea* imprimantei respective în reţea. Pentru aceasta urmaţi calea *clic drept* pe butonul *Start – Control Panel – Hardware and Sound – Devices and Printers.*



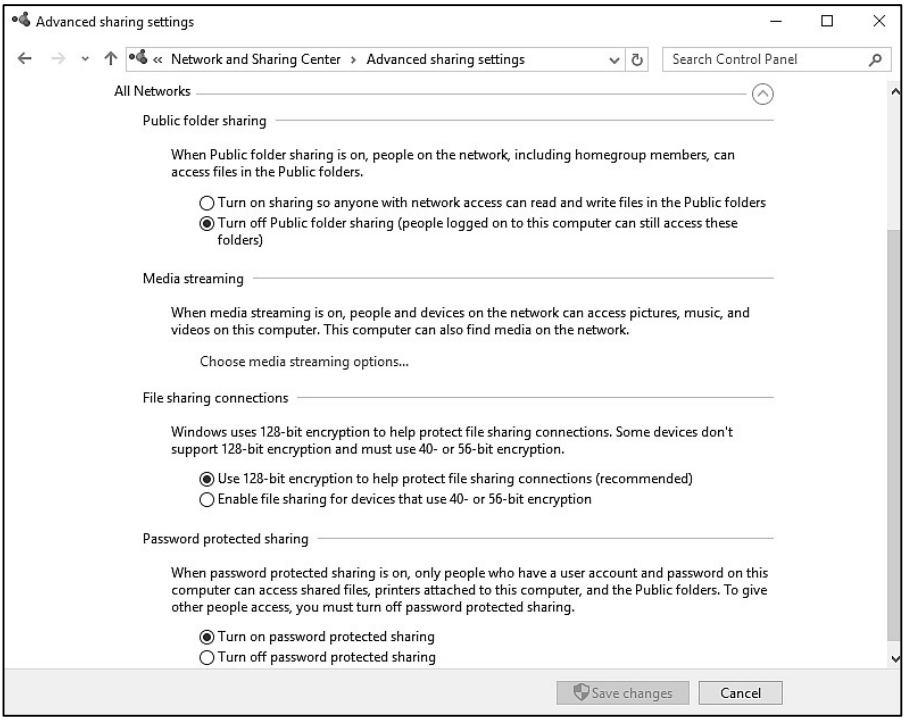
Daţi *clic drept* pe iconul imprimantei care se doreşte a fi partajată (de exemplu *Epson L120* şi alegeţi *Printer properties* în meniul derulant care apare, apoi apăsaţi tabul *Sharing*.

Bifaţi căsuţa *Share this printer* şi alegeţi un nume sugestiv, sub care imprimanta să poată fi recunoscută în reţea (de exemplu *Epson L120 CISS Jet*), apoi apăsaţi butonul *OK*. Acest nume va apărea în lista locală de imprimante.

Pentru a avea acces la imprimantă trebuie să introduceţi *numele utilizatorului* şi *parola* computerului la care este conectată.



Dacă doriți să permiteți accesul la imprimantele partajate dintr-o rețea fără introducerea unei parole, urmați calea *clic drept* pe butonul *Start – Control Panel – Network and Internet – Network and Sharing Center – Change advanced sharing settings*. Va apărea fereastra din pagina următoare:



Alegeți butonul radio *Turn off password protected sharing* și apăsați butonul *Save changes*. Din acel moment orice utilizator din rețea va avea acces nerestricționat la imprimantă, ca și cum ar fi atașată la propriul computer.

Imprimantele care se conectează *direct la rețea* prin cablu cu conectori *RJ45*, vor trebui mai întâi *configurate* conform instrucțiunilor fiecărui producător. După configurare, acestea vor apărea *în listele de impr*imante ale fiecărui utilizator din rețea.

O imprimantă atașată la *HomeGroup* apare în mod automat în lista locală. Când *HomeGroup* este dezactivat, imprimantele atașate devin indisponibile.

Dacă o imprimantă conectată local sau direct la rețea nu apare în *lista locală de imprimante* a unui anumit utilizator, atunci se urmează calea *Start – Settings – Devices – Printers & Scanners – Add a printer or scanner*.

Cele mai recente tipuri de imprimante partajate într-o rețea sunt *imprimantele 3D*, care sunt foarte voluminoase și foarte scumpe.

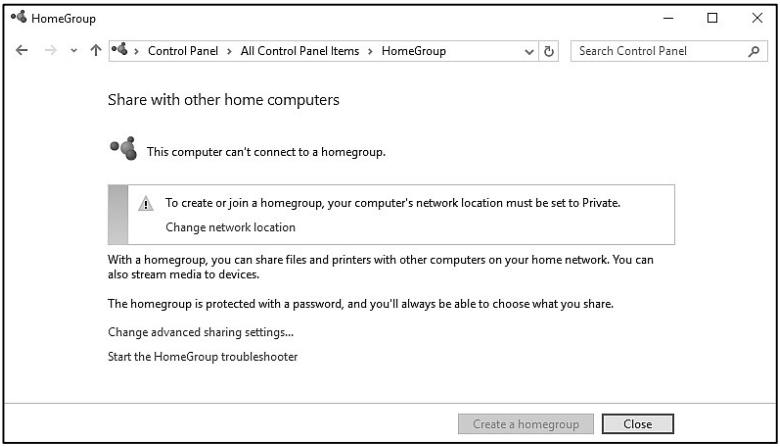
Partajarea cu HomeGroups

HomeGroupurile sunt funcționale doar sub sistemele de operare Windows 7, 8, 8.1 sau 10. De asemenea, acestea sunt funcționale doar dacă rețeaua în care se lucrează este de tip *Home*. Rețelele de tip *Work* sau *Public* nu sunt acceptate, din cauza unor considerente de securitate a datelor.

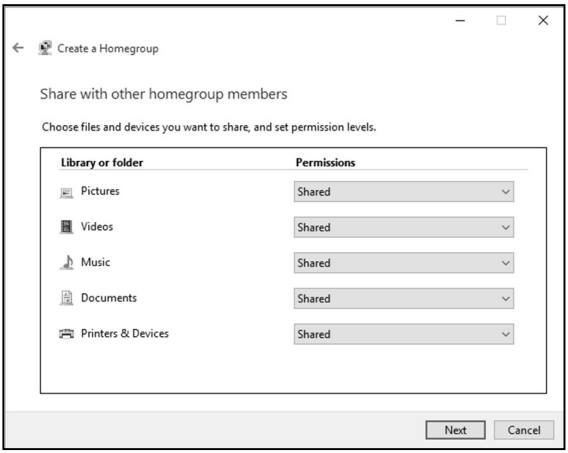
Pentru a afla în ce tip de rețea vă încadrați, urmați calea: clic drept pe *Start – Control Panel – Network and Internet – View network status and tasks* (sub *Network and Sharing Center*). Dacă rețeaua este de tip *Work* sau *Public*, este posibil să nu puteți utiliza *HomeGroup*. De asemenea, HomeGroup poate exista *într-o singură rețea*, dar vă puteți *muta* de la un HomeGroup la altul. *Windows Home Server* este foarte bun pentru managementul HomeGroupurilor.

Pentru a seta un *HomeGroup*, tastați *Home* în căsuța de căutare, apoi alegeți *HomeGroup (Control Panel*) sau urmați calea: *clic drept* pe *Start – Control Panel – All Control Panel Items – HomeGroup.*

Înainte de crea un HomeGroup, computerele trebuie să fie vizibile în rețea. Acest lucru se realizează dând clic pe link-ul *Change advanced sharing settings* și apăsând butoanele *Turn on network discovery, Turn on file and printer sharing* și *Save changes,* apoi se poate apăsa butonul *Create a homegroup.*



În fereastra care apare dați click pe *Next,* iar în fereastra următoare alegeți ce doriți să partajați cu ceilalți membri din *HomeGroup*: imagini, video, muzică, documente, imprimante sau alte dispozitve, după care dați din nou clic pe *Next.*



Windows va genera în mod automat o *parolă complexă*, pe care o puteți nota sau o puteți schimba ulterior urmând calea *Start – Settings – Network & Internet – Homegroup* (dreapta-jos) – *Change the Password*. Înainte de schimbarea parolei asigurați-vă că nu există computere în modul *sleep* sau în *hibernare*.

După schimbarea parolei, trebuie trecut pe la fiecare computer din *HomeGroup* și urmată aceeași cale: *Start – Settings – Network & Internet – Homegroup* (dreapta-jos) – *Change the Password*.

Dacă grupul a fost deja creat, în locul butonului *Create a homegroup* apare butonul *Join now*. În ambele cazuri trebuie să introduceți parola cu care vă conectați la grupul respectiv, apoi dați clic pe butonul *Finish*.

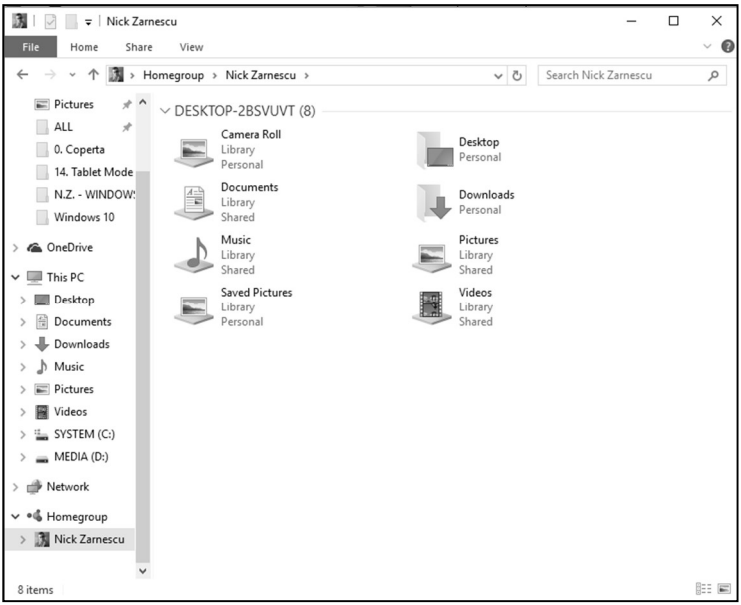
În partea din stânga-jos a lui *File Explorer* apare folderul *Homegroup,* care conține folderele partajate de membrii grupului.

HomeGroup este inclus în mod automat în *Windows Media Player* și apare în panoul de navigare.

În aplicațiile *Office*, HomeGroup poate fi accesat cu *File – Open – Computer – Homegroup*.

Permisiunile la nivel de folder sau fișier pot fi modificate în orice moment (vezi capitolul *Autorizarea accesului la date*).

O *imprimată* atașată unui *computer* care este inclus într-un *HomeGroup* devine, în mod automat, *disponibilă* pentru toți membrii grupului, iar aceștia pot imprima documentele dorite indiferent de locul în care se află.



Setările grupului pot fi modificate cu clic pe folderul *Homegroup*, apoi cu clic pe meniul *HomeGroup*, care apare în partea superioară, urmat de selecția opțiunii *Change homegroup settings*.

Problemele de utilizare ale grupului pot fi rezolvate accesând același meniu, dar selectând, de data aceasta, opțiunea *Start troubleshooter*.

Fișierele individuale pot fi partajate și cu *clic drept* pe acestea, apoi selectarea opțiunii: *Share with* și alegerea dintre alte două opțiuni: *Homegroup (view)* sau *Homegroup (view and edit)*.

Ultima opțiune le permite utilizatorilor grupului să editeze fișierul respectiv, așa că trebuie utilizată cu prudență.

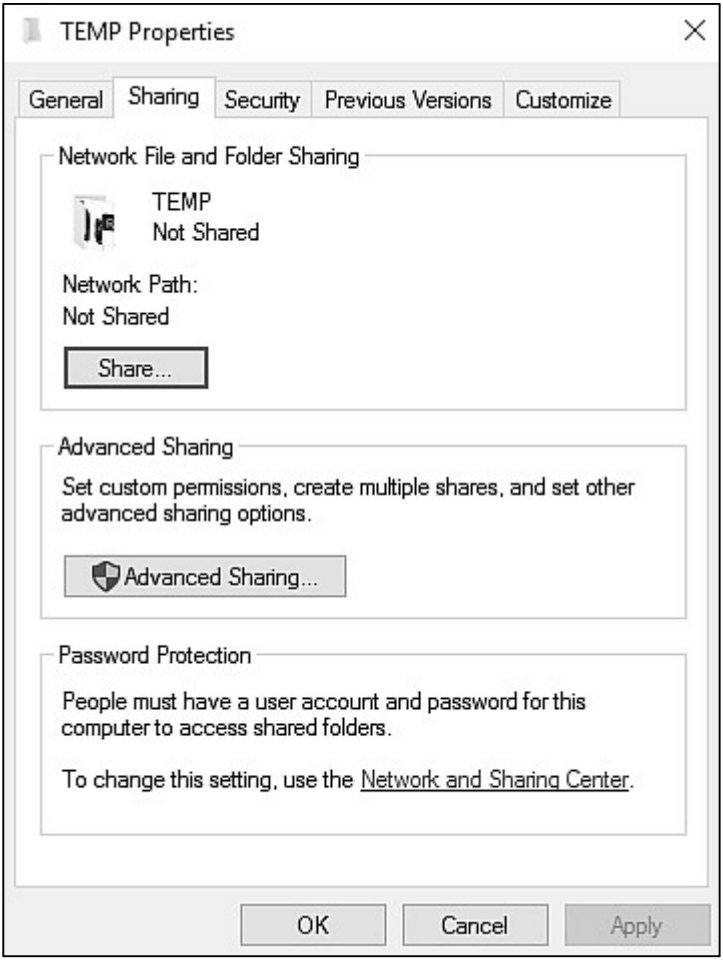
Windows XP sau Vista, în loc de *HomeGroups*, suportă *Workgroups*, care oferă la fel de multe facilități. Cele două tipuri de grupuri pot *coexista*, însă modul de accesare al acestora este diferit.

Un Mac nu poate fi integrat într-un *HomeGroup*, dar poate accesa folderul *\Public* al unui PC. În *Mac OS Finder* alegeți *Go, Connect to Server*. În căsuța *Server Address* tastați *smb://PCName*, apoi apăsați butonul *Connect*. Introduceți numele utilizatorului și parola, iar când vi se solicită nume grupului tastați *workgroup*.

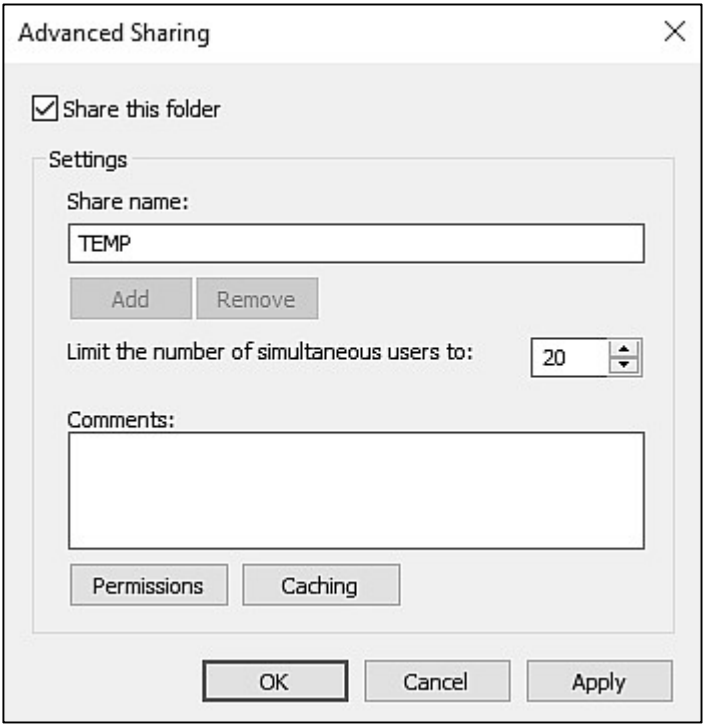
Partajarea folderelor și fișierelor

Partajarea prin rețeaua locală a *folderelor* și *fișierelor* permite accesarea acestora de pe echipamente care rulează atât *Windows 10*, cât și de pe *Mac*-uri, tablete *cu Android* sau *iPhone*-uri.

Pentru a partaja un folder sau un fișier, dați *clic drept* pe folderul sau fișierul respectiv și alegeți *Properties*, apoi apăsați tabul *Sharing*.



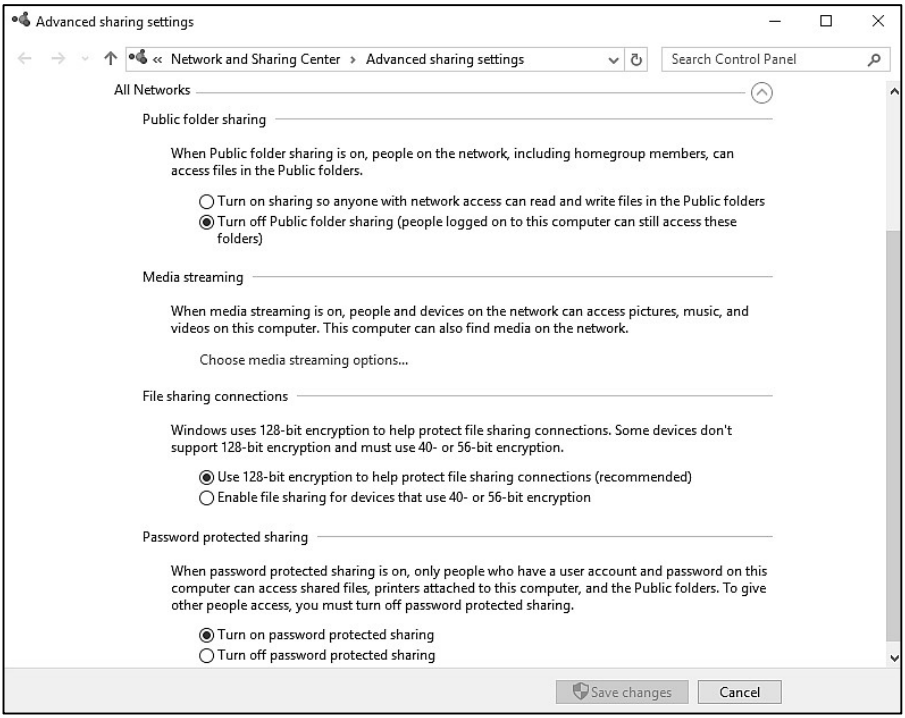
În fereastra *Properties* apăsați butonul *Advanced Sharing* și bifați *Share this folder* în fereastra care apare, apoi apăsați *OK* și *Close*.



Accesul la folderul partajat se face prin intermediul numelui *user*-ului și *parolei* celui care a partajat folderul. Pentru a dezactiva accesul prin credențiale, urmați calea *Start – Settings – Network & Internet – Ethernet – Change advanced sharing options*.

Alegeți butonul radio *Turn off passsword protected sharing* din secțiunea *Password protected sharing*, apoi apăsați butonul *Save changes* (vezi imaginea din pagina următoare).

În mod *implicit*, accesul la folderele și fișierele partajate se face *doar în citire* (read only). Pentru a permite și alte moduri de acces, se setează *permisiuni* de accesare pentru folderele și fișierele respective.

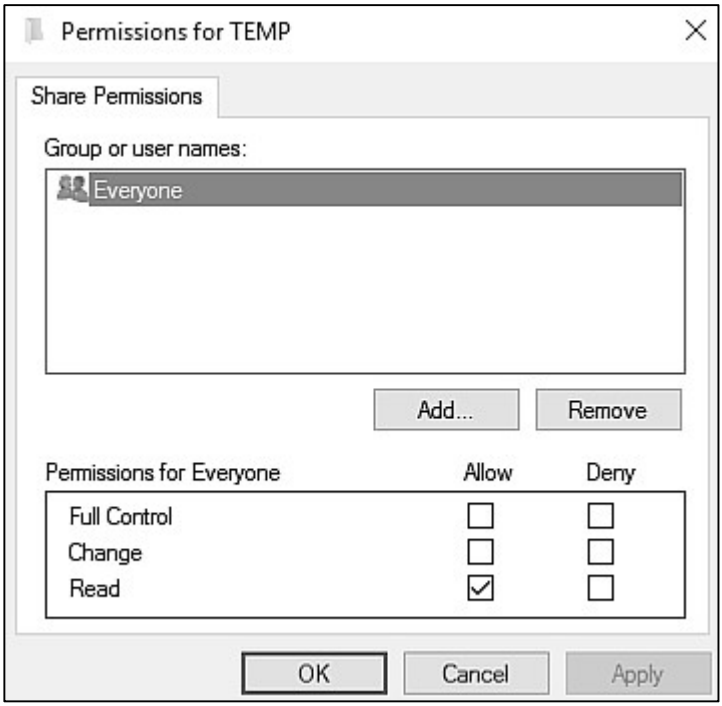


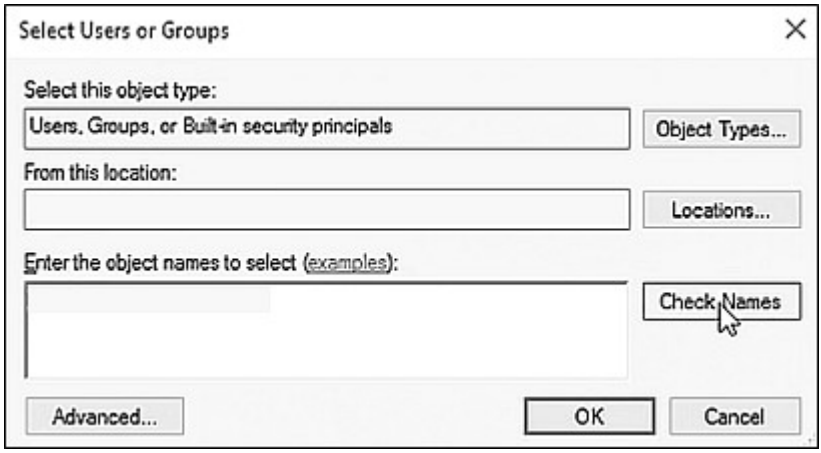
Pentru a stabili tipurile de permisiuni pentru un anumit *utilizator*, dați *clic drept* pe folderul sau fișierul respectiv și alegeți *Properties*, apoi apăsați tabul *Sharing* și butonul *Permissions*. Utilizatorul generic este *Everyone* (oricine). Accesul se permite bifând căsuțele din coloana *Allow* sau poate fi interzis bifând căsuțele din coloana *Deny*.

Un *utilizator* nou sau un *grup* nou pot fi adăugați apăsând butonul *Add*. În fereastra *Select users or groups* se introduce numele obiectului care se dorește adăugat și se apasă butonul *Check Names*, pentru a verifica dacă tastarea a fost efectuată în mod corect.

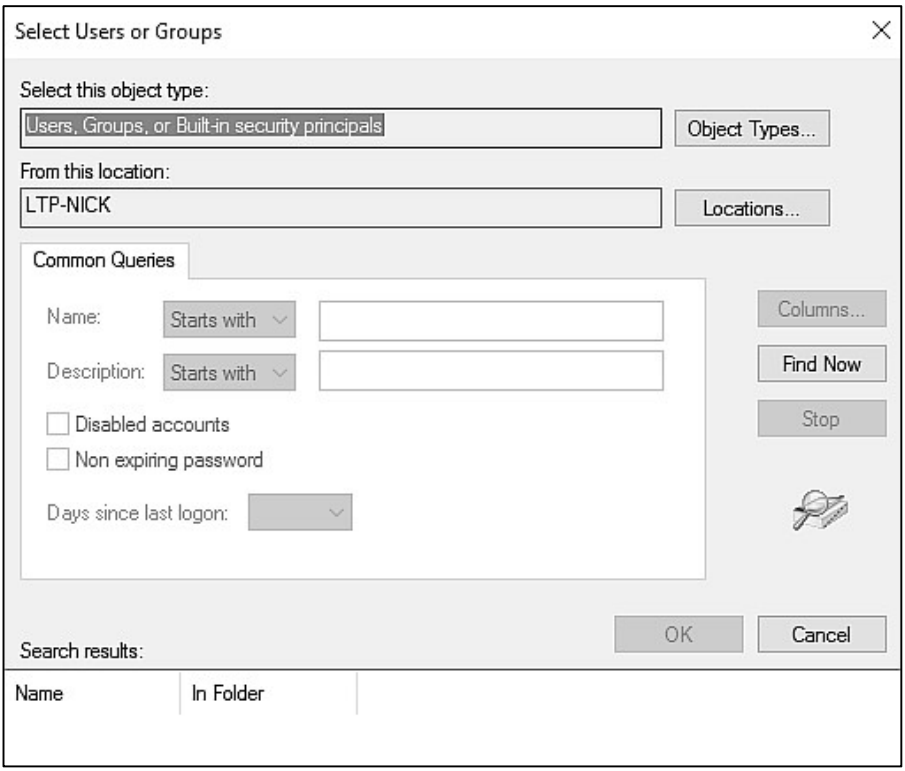
Dacă numele utilizatorului sau al grupului au fost introduse *corect*, după apăsarea butonului *Check Names*, acestea apar *subliniate* în partea inferioară.

După ce ați apăsat butonul *OK*, veți observa apariția grupului sau user-ului în căsuța *Group or user names*. Apăsați din nou butonul *OK*, apoi butonul *Close*, în fereastra principală.


Permissions for TEMP
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply


Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel

Permisiuni avansate asupra utilizatorilor sau grupurilor pot fi acordate apăsând butonul *Advanced* din fereastra *Select Users or Groups* (vezi pag. 115 jos).



Managementul accesului la date

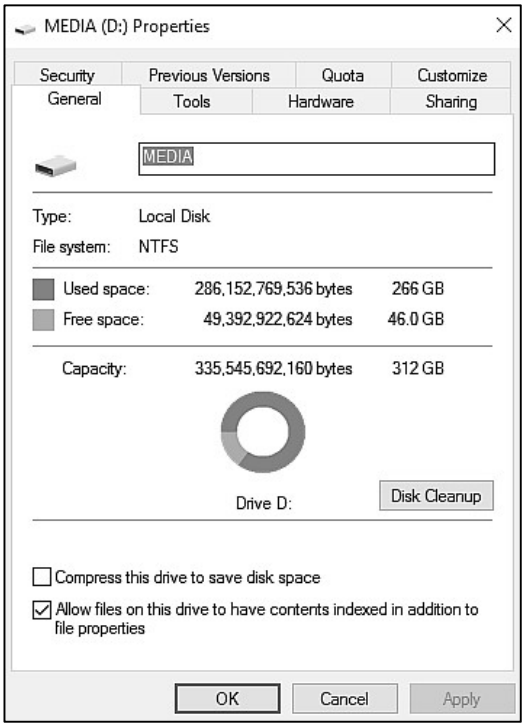
Alocarea spațiului pe drive-uri sau partiții
Managementul folderelor cu File Explorer
Utilizarea bibliotecilor
Redirecționarea bibliotecilor
Auditul folderelor și fișierelor

Alocarea spațiului pe drive-uri sau partiții

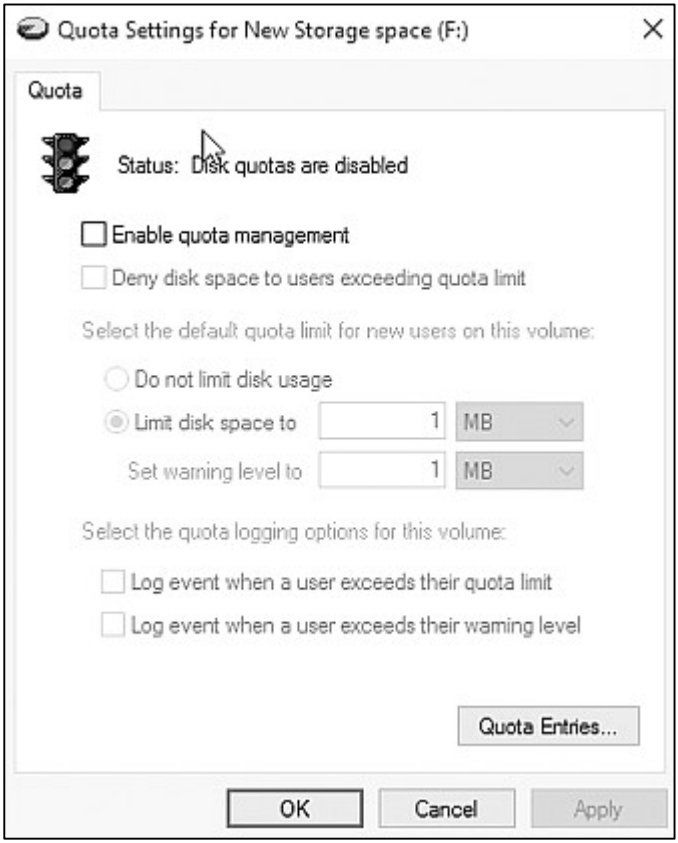
În cazul în care un computer este accesat de mai mulți utilizatori, se poate aloca, pentru fiecare utilizator, o anumită *cotă* (quota) din drive-ul sau partiția respectivă, în următoarele condiții:

- Alocarea cotelor se poate face doar de către *administratorul* computerului;
- Drive-ul sau partiția trebuie să fi fost formatate anterior în *NTFS*;
- Cotele se pot aloca doar pentru *drive*-uri și *partiții*, nu și pentru foldere;
- Cotele *nu se pot aloca simultan* pentru mai multe drive-uri sau partiții;
- Utilizatorul nu mai poate utiliza alt spațiu când atinge *dimensiunea maximă* a cotei sau după ce primește un *avertisment* că în curând va depăși cota.

Pentru a stabili o cotă, vă logați ca *administrator*, dați *clic drept* pe *partiția* în care vreți să fixați cota, alegeți *Properties*, apoi apăsați tabul *Quota*.



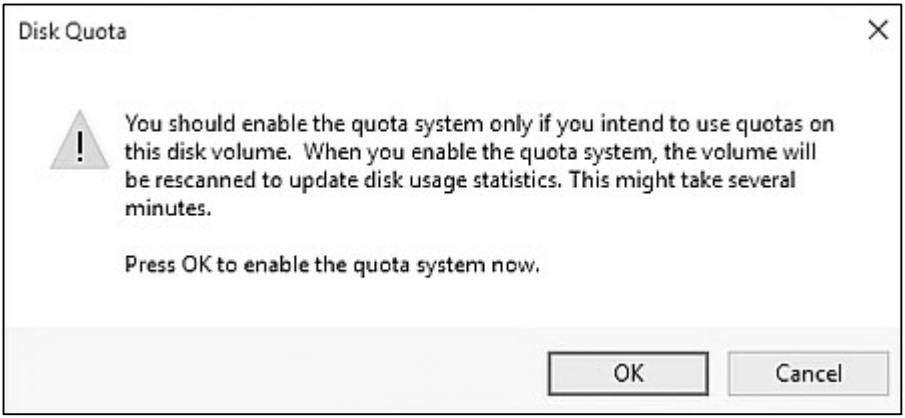
În fereastra care apare, apăsați butonul *Show Quota Settings*, apoi bifați căsuța *Enable quota management*. Dacă bifați și *Deny disk space to users exceeding quota limits*, atunci uilizatorul nu mai poate utiliza alt spațiu în afara cotei.



În cazul nostru partiția are 102GB și va fi accesată de doi membri ai familiei, fiecare având alocată o cotă de 51GB. Apăsați butonul radio *Limit disk space to* și introduceți valoarea 51, iar din meniul derulant alegeți *GB*. În căsuța *Set warning level to* introduceți 50 și alegeți din nou GB.

Fiecare din cei doi utilizatori vor putea accesa câte 51GB din partiția D: (MEDIA), iar când vor atinge limita de 50GB, vor primi o notificare în acest sens.

Apăsați butonul *Apply*. Veți primi un mesaj de avertisment prin care vi se comunică faptul că *activarea* cotei necesită o *rescanare* a partiției, proces care ar putea dura mai multe minute, în funcție de dimensiunea partiției.



Apăsați *OK* în această fereastră, apoi *OK* în ferestra *Quota Settings for New Storage space* și din nou *OK* în fereastra *Properties*.

Puteți testa funcționarea cotei copiind mai multe filme de dimensiuni mari (2-4GB), până atingeți *cota de avertizare*, apoi le ștergeți.

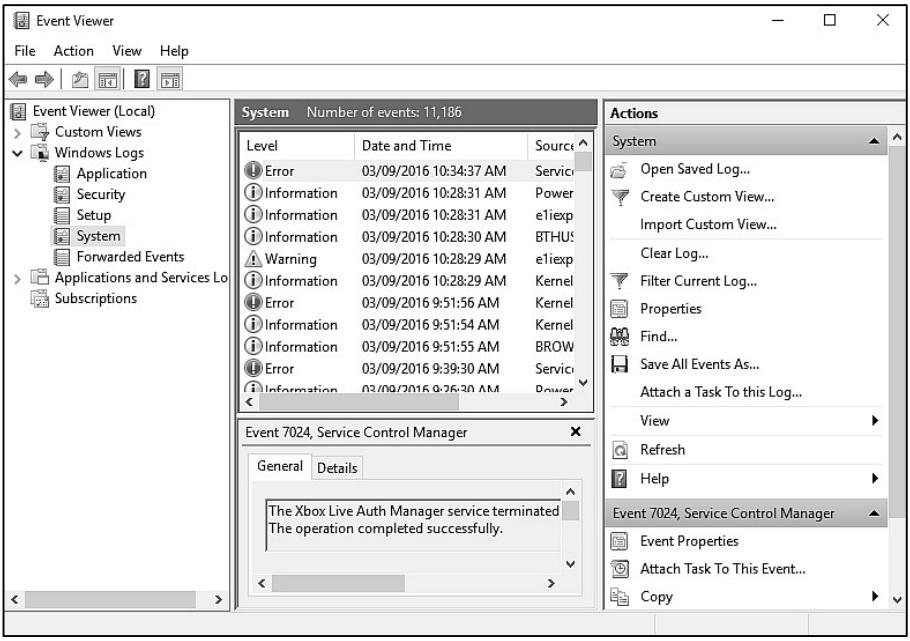
Dacă în ferestra *Quota Settings for New Storage space* veți bifa și căsuțele *Log event when a user exceeds their quota limit* și *Log event when a user exceeds their cota limit*, atunci evenimentele de atingere a cotei de avertizare și a dimensiunii maxime a cotei vor fi înregistrate într-un fișier log, care poate fi vizualizat cu *Event Viewer*.

Apăsați *OK* în ferestra *Quota Settings for New Storage space* și din nou *OK* în fereastra *Properties*.

Pentru a vizualiza evenimentele cu *Event Viewer*, tastați *event* în căsuța de căutare pentru Cortana și aleți *Event Viewer (Desktop app)*.

În panoul din stânga, expandați *Windows Logs* și dați clic pe *System*. Dacă în panoul central, coloana *Source*, nu vedeți *NTFS*, atunci, în panoul din dreapta, dați clic pe *Find* și tastați *NTFS* în căsuța de căutare, apoi apăsați butonul *Find Next*. Dacă dați clic pe *evenimentul* respectiv, în partea de jos a panoului central veți găsi o *explicație amănunțită* a acestuia.

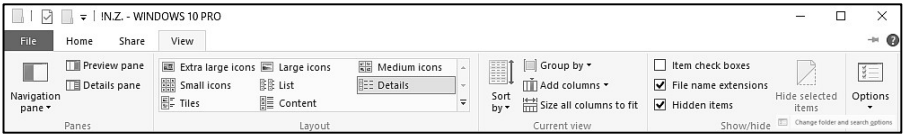
Informațiile despre evenimente pot fi copiate *cu Action – Copy – Copy Details as Text*, apoi lipite într-un fișier creat cu *Word*, *Excel* sau *Notepad*.

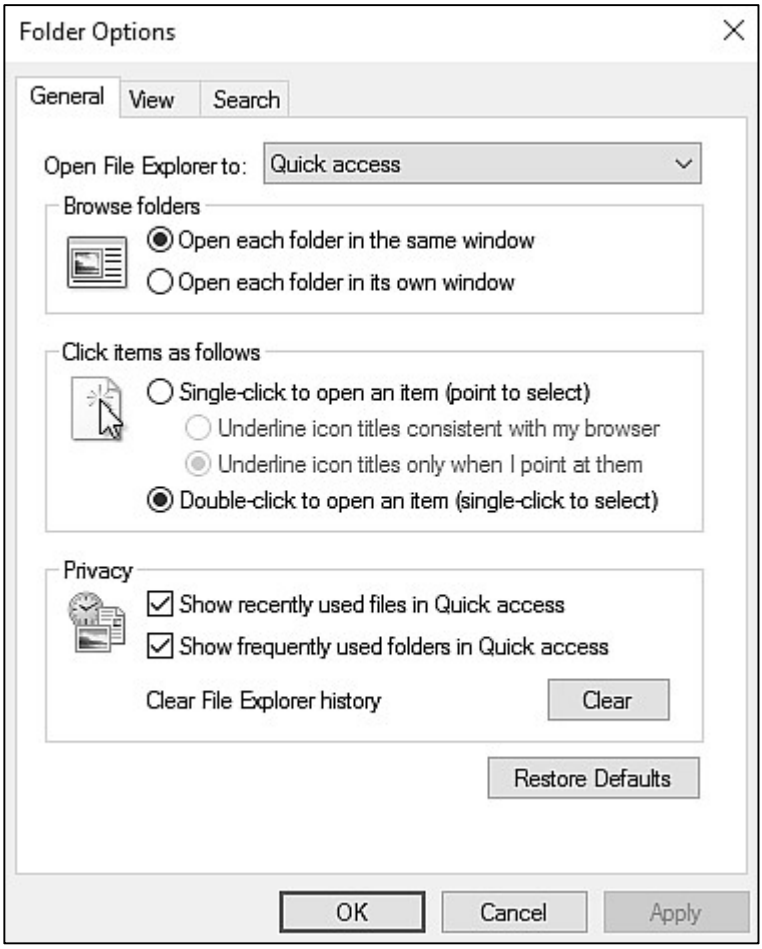


Managementul folderelor cu File Explorer

Pentru a configura opțiunile pentru foldere în Windows 10, deschideți *File Explorer*, dați clic pe tabul *View* al meniului orizontal din partea superioară, clic pe caseta *Options*, iar din meniul derulant care apare alegeți *Change folder and search options*.

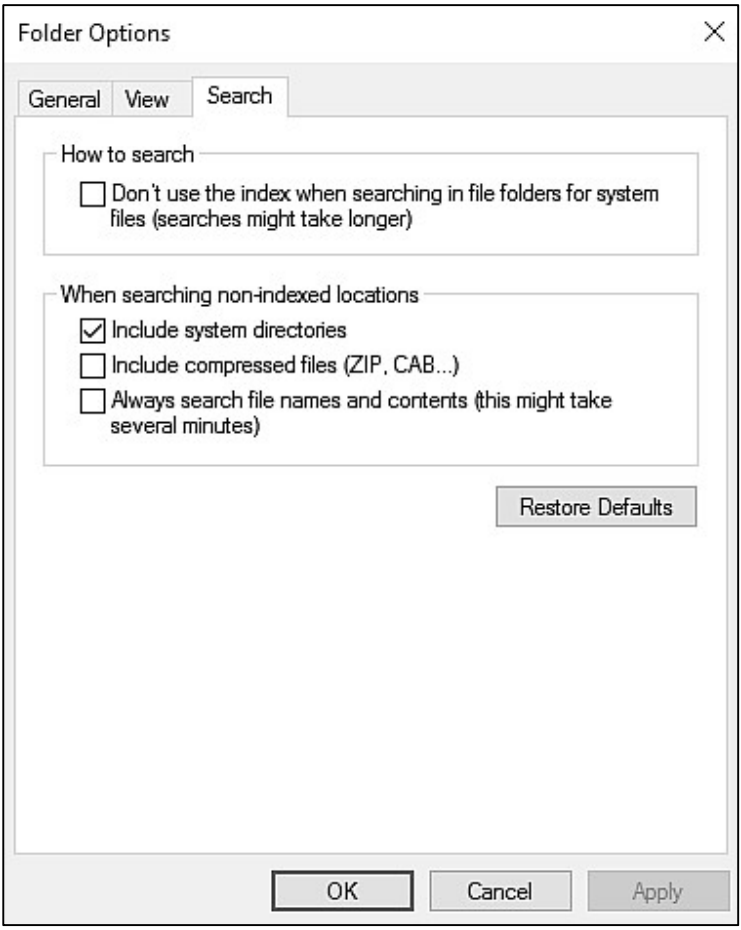
Se va deschide o fereastră cu trei taburi: *General, View* și *Search* (vezi pagina următoare. Taburile *General* și *Search* sunt foarte simple și nu necesită o tratare amănunțită. Tabul *View* este foarte complex și-l vom studia în detaliu.





Deoarece această carte se adresează profesioniștilor, se presupune că aceștia au cunoștințe minime de limba engleză și doar vor alege butoanele radio dorite sau vor bifa căsuțele care-i interesează.

Quick access este nou în Windows 10, dar a fost prezentat în detaliu în volumul anterior „*Windows 10 Ghid practic*". Vom mai aminti despre acesta și în paginile care urmează.



Aceeași precizare se poate face și pentru tabul *Search*. O opțiune foarte utilă, dar mare consumatoare de timp, ar fi bifarea căsuței *Always search file names and contents*. Dacă ați rătăcit un fișier pe hard disk, dar știți sigur că acesta conține un anumit cuvânt (de exemplu *redundanță*), bifați căsuța respectivă și efectuați căutarea cu *File Explorer*, tastând *redundanță* în căsuța *Search* din dreapta-sus. În rezultatele căutării ar trebui să se afle și fișierul dorit.

Multe din opțiunile tabului *View* sunt cunoscute din versiunile anterioare de Windows: 7, 8 sau 8.1.

O opțiune interesantă este bifarea căsuței *Show encrypted or compressed NTFS files in color*. Fișierele NTFS criptate sau compresate vor apărea afișate în *File Explorer* cu o anumită *culoare*, în loc de negru, cum este în mod obișnuit.

Altă opțiune, la fel de interesantă, este bifarea căsuței *Use Sharing Wizard*, care este *activă* în mod *implicit* și despre care vom vorbi ulterior în detaliu.

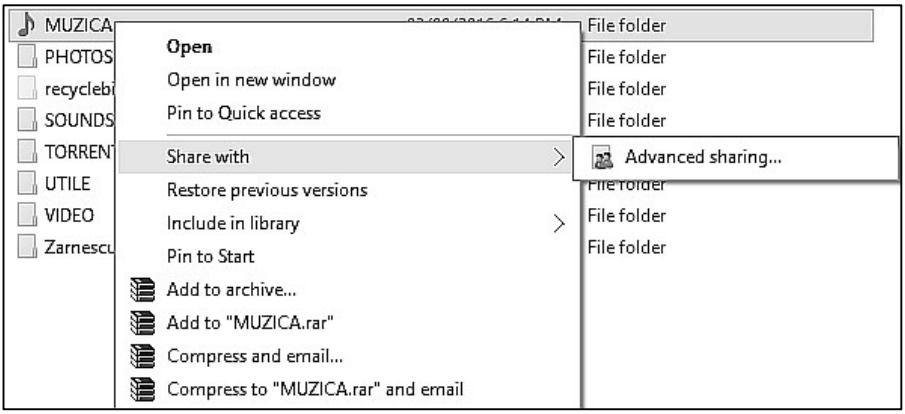
Secțiunea *Navigation Pane* este introdusă de Windows 10 și se referă la panoul de navigare, din partea stângă a lui *File Explorer*.

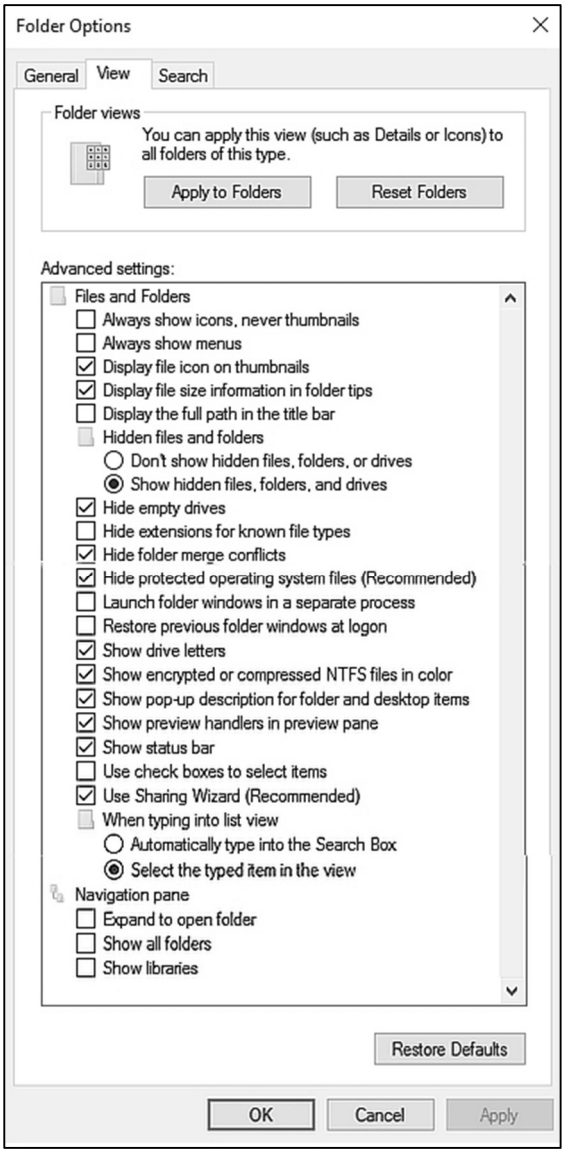
Dacă bifați *Expand to open folder*, va fi expandat folderul care este selectat în panoul de navigare. Cu *Show all folders* vor fi afișate toate folderele din panou (inclusiv folderul *Libraries*), iar cu *Show libraries* va fi afișat folderul *Libraries* în partea din stânga-jos a panoului de navigare, cu următoarele subfoldere: *Camera Roll*, *Documents*, *Music*, *Pictures, Saved Pictures* și *Videos*.

Opțiunea *Use Sharing Wizard* este introdusă de Windows 10 și este *activă* în mod implicit. Dacă vreți să *partajați un folder* cu prietenii, dați *clic drept* pe folderul respectiv (de exemplu D:\MUZICA) și selectați *Share with*. Va apărea următorul meniu vertical:



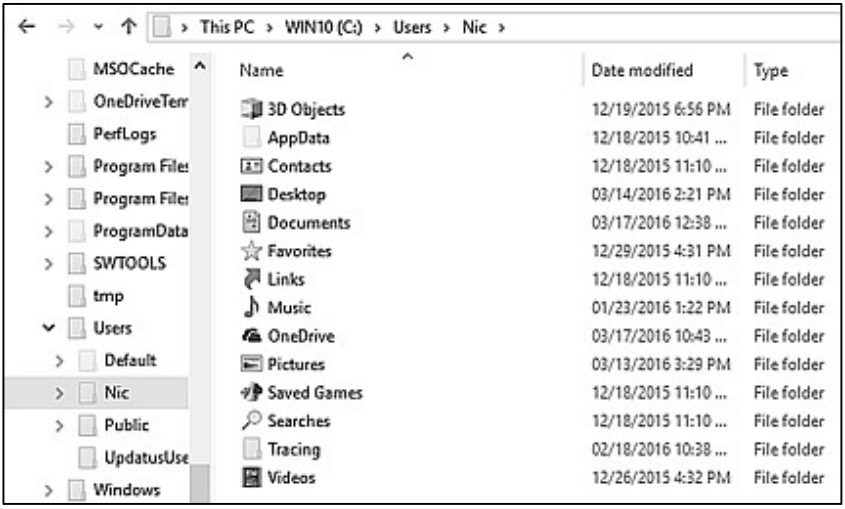
Dacă opțiunea este *debifată*, atunci când veți da *clic drept* pe folderul dorit și pe *Share with*, va apărea un meniu cu o singură opțiune: *Advanced sharing*. De fapt aceasta este opțiunea *implicită* dacă doriți să partajați *imprimante*, *stick*-uri sau *drive*-uri pe USB.




Folder Options
General
View
Search
Folder views
You can apply this view (such as Details or Icons) to all folders of this type.
Apply to Folders
Reset Folders
Advanced settings:
Files and Folders
Always show icons, never thumbnails
Always show menus
Display file icon on thumbnails
Display file size information in folder tips
Display the full path in the title bar
Hidden files and folders
Don't show hidden files, folders, or drives
Show hidden files, folders, and drives
Hide empty drives
Hide extensions for known file types
Hide folder merge conflicts
Hide protected operating system files (Recommended)
Launch folder windows in a separate process
Restore previous folder windows at logon
Show drive letters
Show encrypted or compressed NTFS files in color
Show pop-up description for folder and desktop items
Show preview handlers in preview pane
Show status bar
Use check boxes to select items
Use Sharing Wizard (Recommended)
When typing into list view
Automatically type into the Search Box
Select the typed item in the view
Navigation pane
Expand to open folder
Show all folders
Show libraries
Restore Defaults
OK
Cancel
Apply

Utilizarea bibliotecilor

Subfolderele din folderul *Libraries* sunt de fapt virtuale, deoarece conținutul lor se află în *C:\Users\nume_user* și în *C:\Users\Public* sau pe *OneDrive*. O bibliotecă poate fi redirecționată și spre un folder dintr-o altă partiție, după cum vom vedea în pagina următoare. Dacă există mai multe conturi de utilizator pe același computer, fiecare va avea bibliotecile sale.

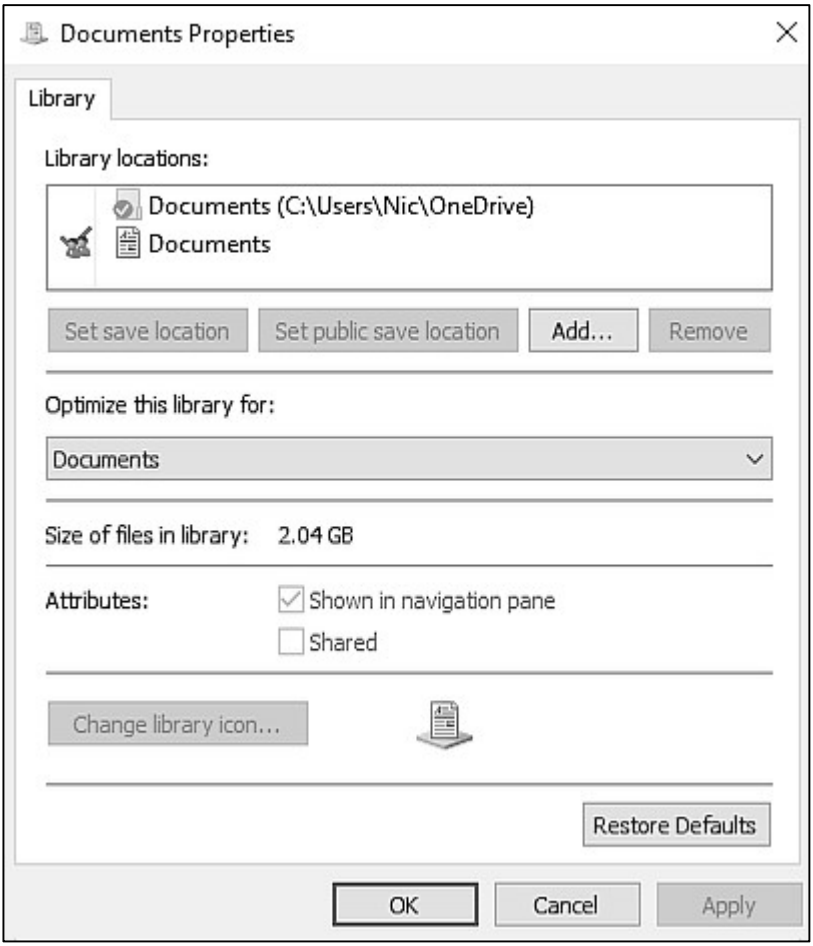


Un subfolder din *Libraries*, de exemplu *Documents*, poate să conțină trei foldere: unul care se află în *C:\Users\nume_user*, unul pe *OneDrive* și unul pe partiția *D:* sau pe oricare altă partiție.

Un mare avantaj al bibliotecilor este acelea că sunt *indexate automat* de Windows 10, ceea ce face mult mai rapid procesul de căutare a fișierelor.

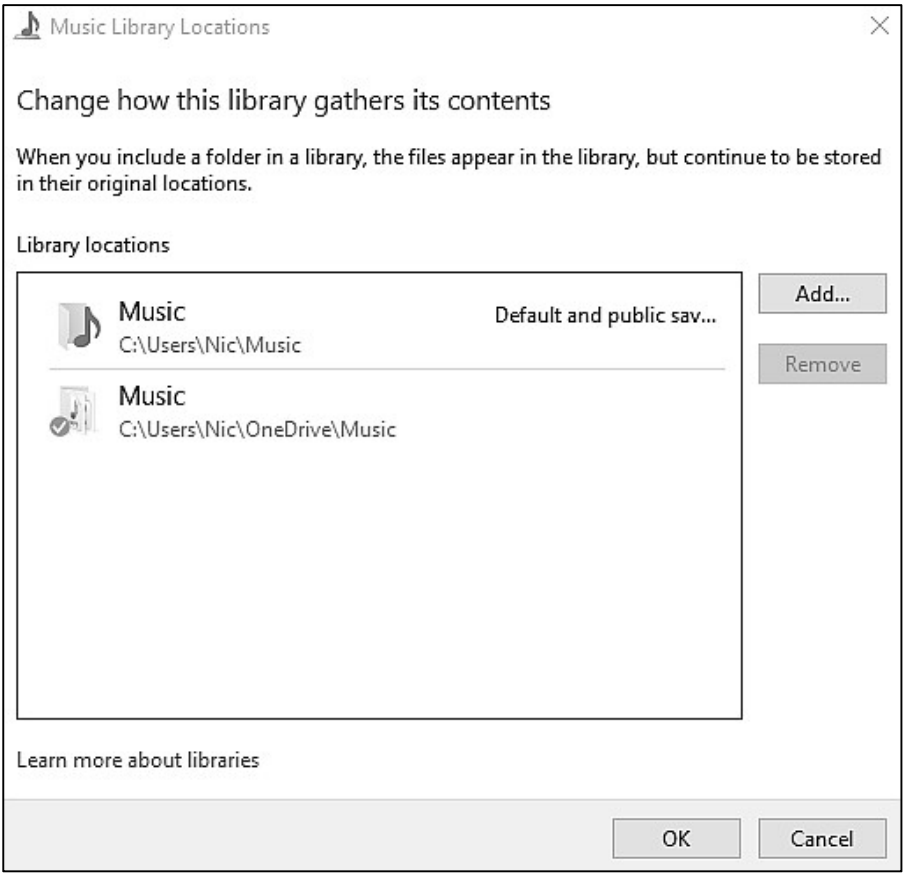
Pentru a crea o nouă bibliotecă, se dă clic drept pe *Libraries*, se alege *New* din meniul vertical, apoi *Library*. Puteți să creați un folder nou în *Libraries*, dând clic drept pe folderul respectiv (de exemplu *D:\CĂRȚI*) și alegând *Include în library* din meniul vertical care apare.

Pentru a *șterge* un subfolder din Libraries, să dă *clic drept* pe acesta și se alege *Remove location from library*. Puteți adăuga sau șterge foldere și dacă dați *clic drept* pe folderul respectiv, selectați *Properties*, apăsând apoi butonul *Add* sau *debifați* căsuța folderului din secțiunea *Library locations* și apăsați butonul *Remove*.



Cu butoanele *Set save location* şi *Set public save location* se pot schimba locurile reale în care vor fi stocate conţinuturile folderelor.

Un management complex al bibliotecilor se poate realiza deschizând *File Explorer*, selectând biblioteca respectivă şi apăsând tabul *Manage* din dreapta-sus, apoi *Manage library* din stânga-sus (vezi pagina următoare).



Când se include un folder într-o bibliotecă, datele se stochează, în continuare, în folderul original. Cu clic pe un folder din secțiunea *Library locations* se poate schimba locul de pe hard disk în care se memorează conținutul acestuia.

Cu butoanele *Add* și *Remove* se pot adăuga sau șterge foldere în sau din bibliotecă.

Redirecționarea bibliotecilor

Bibliotecile din Windows 10 sunt *Documents, Downloads, Music, Pictures* și *Videos*, accesul lor realizându-se din *panoul de navigare* al lui *File Explorer* (sub *This PC*).

Aceste biblioteci se găsesc pe *partiția C* (sistem) și, cu timpul, pot deveni neîncăpătoare, încetinind sau chiar blocând sistemul de operare.

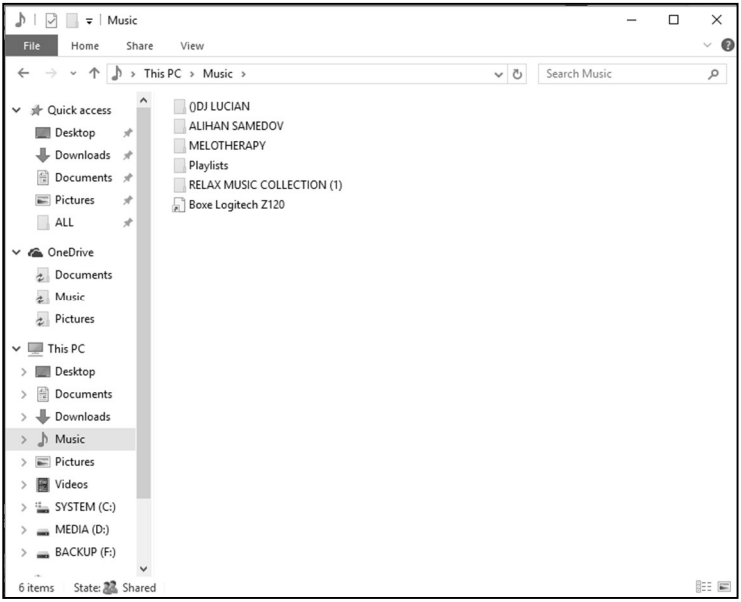
O soluție ar fi mutarea acestor biblioteci pe partiția D sau pe altă partiție disponibilă. În acest mod se îndeplinesc două deziderate: partiția C va conține doar *sistemul de operare* și *aplicațiile instalate*, iar *Groove Music*, *Photos* și *Movies & TV* vor fi direcționate către aceste biblioteci.

Redirecționarea bibliotecilor se face prin *clic drept* pe acestea, selectare *Properties* și acționarea tabului *Location*.



În cazul nostru, biblioteca *Music* a fost redirecționată către folderul *D:\MUZICA*. În fereastra *Properties* mai există alte cinci taburi, prin care se pot realiza setări avansate: *General, Previous Versions, Customize, Sharing* și *Security*.

Autorul a redirecționat bibliotecile de pe computerul său astfel: *Documents* în D:\DOC, *Downloads* în D:\DOWNLOADS, *Music* în D:\MUZICA, *Pictures* în D:\FOTO și *Videos* în D:\FILME.



Toate descărcările (*downloads*) se vor face în partiția D, *documentele* vor exista în aceeași partiție, iar aplicațiile *Groove Music*, *Photos* și *Movies & TV* se vor actualiza automat cu conținutul folderelor D:\MUZICA, D:\FOTO și D:\FILME.

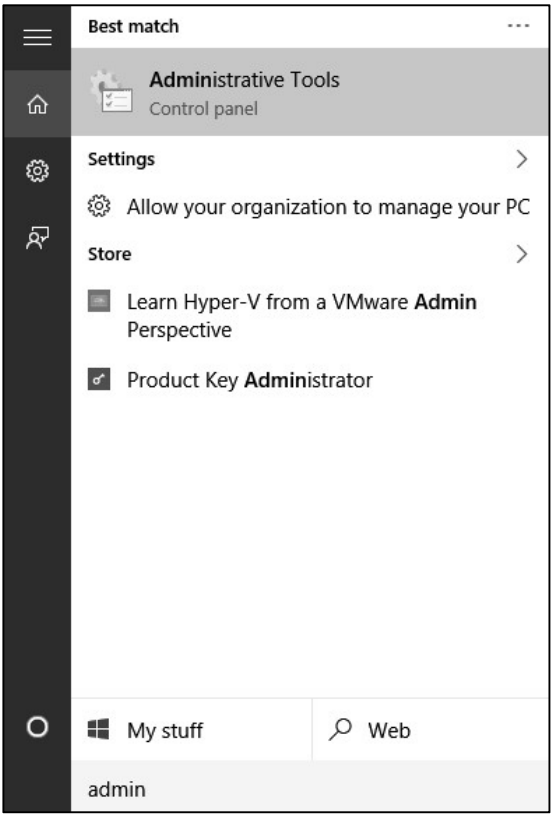
Reamintim că aplicațiile *Groove Music* și *Photos* includ și conținutul folderelor *Music* și *Pictures* de pe *One Drive*, care poate fi accesat doar dacă v-ați logat cu un cont Microsoft.

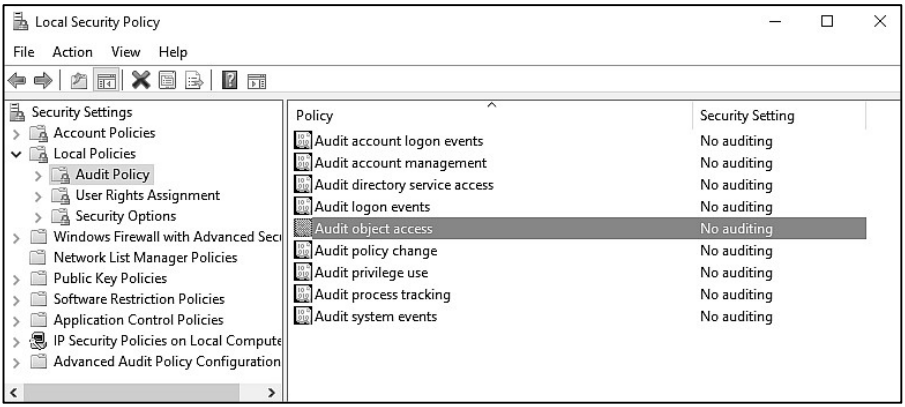
Auditul folderelor și fișierelor

Când se lucrează într-o rețea de calculatoare, este foarte important pentru un administrator să știe cine a *creat*, *citit*, *modificat* sau *șters* un anumit fișier..

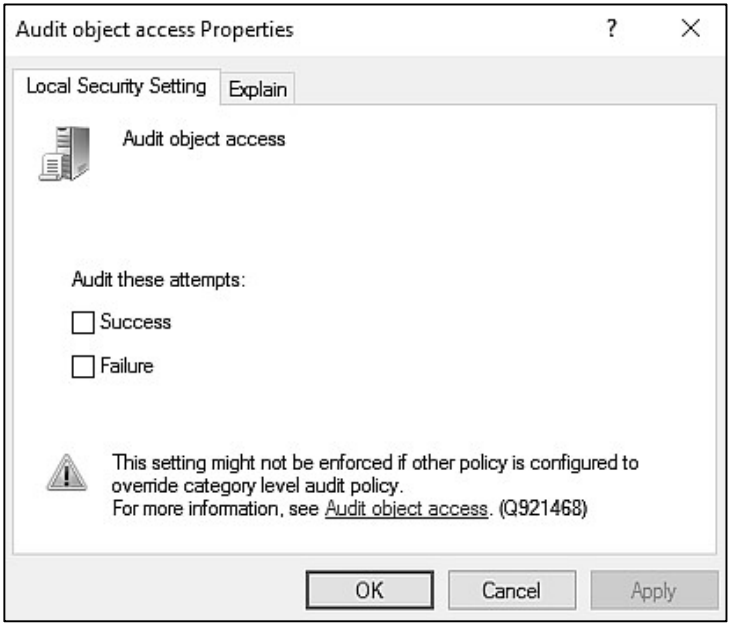
Pentru a putea realiza acest lucru, administratorul de rețea trebuie să activeze opțiunea de *audit al fișierelor* pe *file server*, pe *folderele* și pe *fișierele* de importanță majoră de pe stațiile (workstations) cu Windows 10, urmărind apoi cu *Event Manager* și interpretând evenimentele de sistem care apar.

Activarea auditului fișierelor pe computerul cu Windows 10 se face tastând *admin* în căsuța de căutare pentru Cortana, alegând *Administrative Tools (Control Panel)*, apoi selectând *Local Security Policy*.





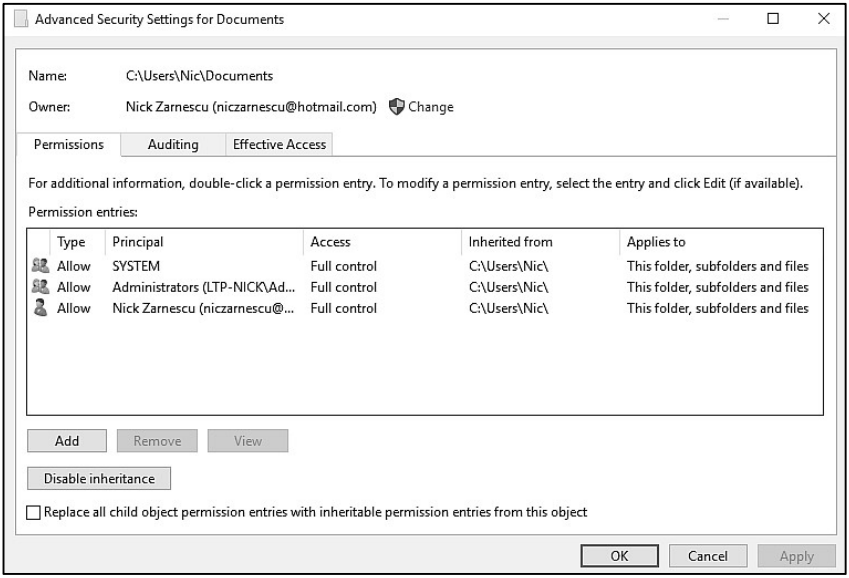
În fereastra *Local Security Policy* expandați *Local Policies* și selectați *Audit Policy*, iar în panoul din dreapta dați clic pe *Audit object access*. În meniul orizontal superior apăsați *Action*, apoi selectați *Properties*.



În fereastra care apare bifați *Success* și *Failure*, apoi apăsați butonul *OK* și închideți fereastra *Local Security Policy*.

Deschideți acum *File Explorer,* dați clic drept pe folderul *Documents*, apoi alegeți *Properties* și apăsați tabul *Security*.

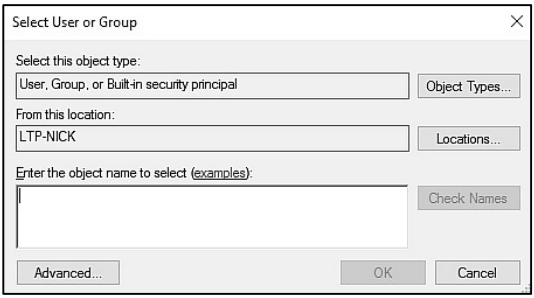
În fereastra *Documents Properties* apăsați butonul *Advanced*, tabul *Auditing* și butoanele *Continue*, apoi *Add*.

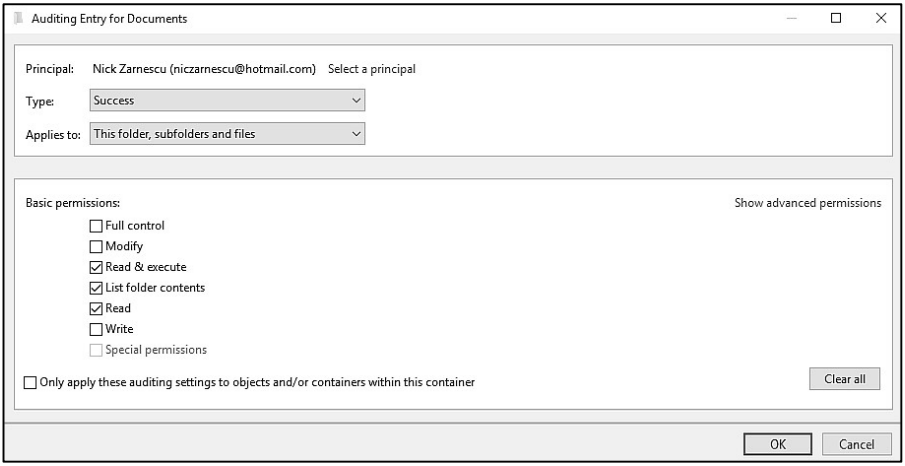


În fereastra *Auditing Entry for Documents*, singura opțiune care poate fi accesată este *Select a principal*. În fereastra *Select User or Group* se introduc *numele grupului* sau *numele utilizatorului* asupra cărora se dorește auditul.

Corectitudinea numelor introduse poate fi verificată cu butonul *Check Names*. Dacă acestea sunt corecte, după apăsarea butonului vor apărea subliniate cu o linie inferioară continuă. Pentru continuare apăsați *OK.*

Fereastra *Auditing Entry for Documents* devine acum complet accesibilă.





În partea superioară alegeți alegeți *Type: All* și bifați căsuța *Full control* în secțiunea *Basic permisions* sau bifați doar căsuțele care va interesează pentru auditul folderelor și fișierelor.

Se poate proceda identic și cu alte foldere (nu doar cu *Documents*), în funcție de interesul pe care-l manifestați în efectuarea auditului.

Salvare și restaurare

Backup și Restore

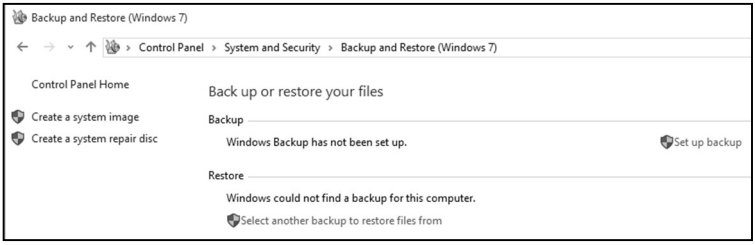
Pentru a evita pierderile importante de date în cazul unei defecțiuni *hardware* (hard disk) sau *software* (Windows 10), Microsoft recomandă utilizarea operațiunilor de *Backup* (salvare) și *Restore* (restaurare).

Backup-ul *complet* realizează salvarea *fișierelor personale* de pe computer, împreună cu *sistemul de operare*. După remedierea defecțiunii, acestea pot fi restaurate și sistemul de operare devine perfect funcțional, iar fișierele sunt recuperate integral.

Backup-ul *File History* realizează doar salvarea *fișierelor individuale*, fără sistemul de operare.

În ambele cazuri, backup-ul se va face pe un hard disk extern, formatat în NTFS, care va fi utilizat doar pentru această operațiune și care va avea o capacitate superioară hard diskului din PC.

Backupul complet se realizează urmând calea: click drept pe *Start – Control Panel – System and Security – Backup and Restore (Windows 7) – Set up Backup* sau *Create a system image.*

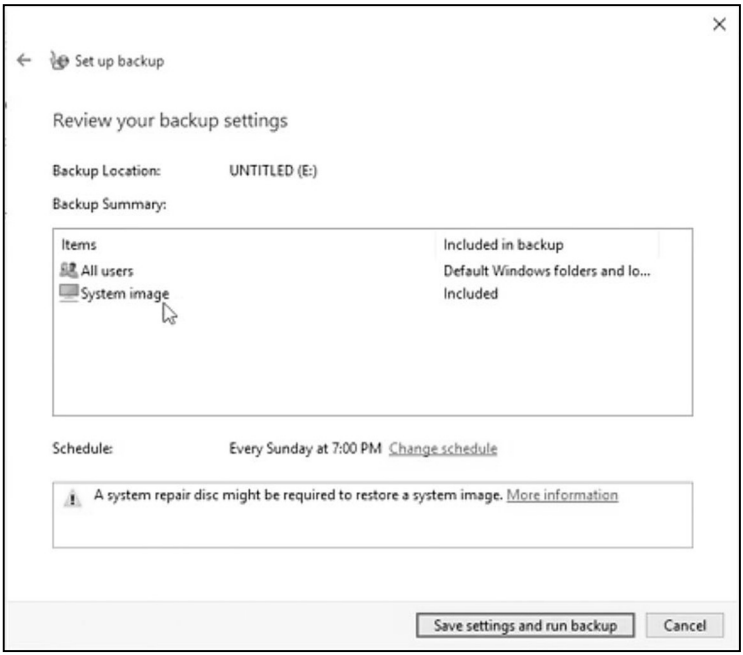


Dacă ați selectat *Set up a backup*, alegeți hard diskul extern pe care se va efectua salvarea și dați clic pe *Next*. Aveți de ales între două opțiuni: *Let Windows choose (recommended)* sau *Let me choose*. Prima opțiune este mai sigură, așa că puteți da clic pe *Next*.

Se observă că vor fi salvate toate *fișierele personale* ale utilizatorilor care accesează PC-ul respectiv, împreună cu *imaginea sistemului de operare*.

Periodicitatea salvării, *ziua* și *ora* pot fi modificate selectând opțiunea *Change schedule*.

Lansarea backup-ului se face cu *Save settings and run backup*.



Primul backup va avea o durată mai mare, backupurile ulterioare salvând doar modificările față de cel anterior.

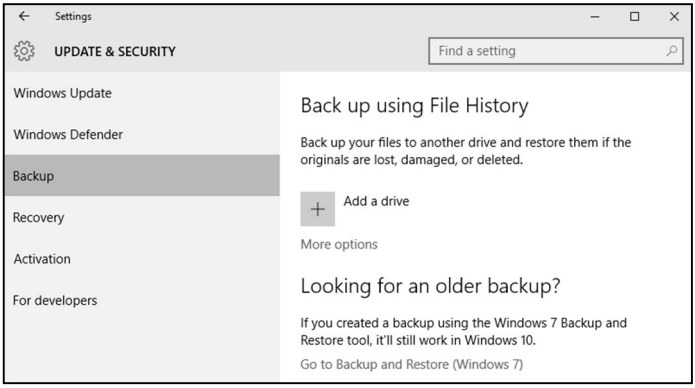
Puteți lăsa hard diskul extern conectat la PC și backupurile se vor face în background în ziua și la ora stabilită, fără intervenția utilizatorului sau puteți deconecta, pentru siguranță, hard diskul extern, pe care-l veți reconecta cu puțin înainte de pornirea backupului.

Dacă a apărut o problemă de funcționare, conectați drive-ul extern pe care ați efectuat backup-ul și urmați calea: click drept pe *Start – Control Panel – System and Security – Backup and Restore (Windows 7) – Restore my files* sau *Restore all user's files.* Ultimele două opțiuni apar doar dacă ați conectat hard diskul extern.

Se recomandă efectuarea periodică a ambelor backup-uri (*complet* și *File History*).

File History

File History permite salvarea fișierelor personale (*Desktop*, *Libraries*, *Contacts* și *Favorites*). Se urmează calea: *Start – Settings – Update & Security – Backup.*



Se conectează hard diskul extern și se dă clic pe *Add a drive* . Se verifică poziția pe *On* a comutatorului *Automatically back up my files*, apoi se dă clic pe *More options*.

În fereastra *Backup Options* care apare se pot adăuga folderele care vor fi salvate (*Add a folder*), alături de cele standard, asociate fiecărui utilizator.

Dacă nu se dorește salvarea anumitor subfoldere, în secțiunea *Exclude these folders*, se selectează *Add a folder*. Dacă nu se dorește salvarea unui întreg folder, se selectează din listă folderul respectiv și se dă clic pe butonul *Remove*.

În secțiunea *Overview* din Backup Options se pot stabili *periodicitatea* backupului (*Backup my files* – minute, ore, zile) și *durata de păstrare* a acestuia (*Keep my backups* – permanent, luni, ani, până la epuizarea spațiului de stocare). Pentru a demara salvarea fișierelor, se dă clic pe butonul *Back up now*.

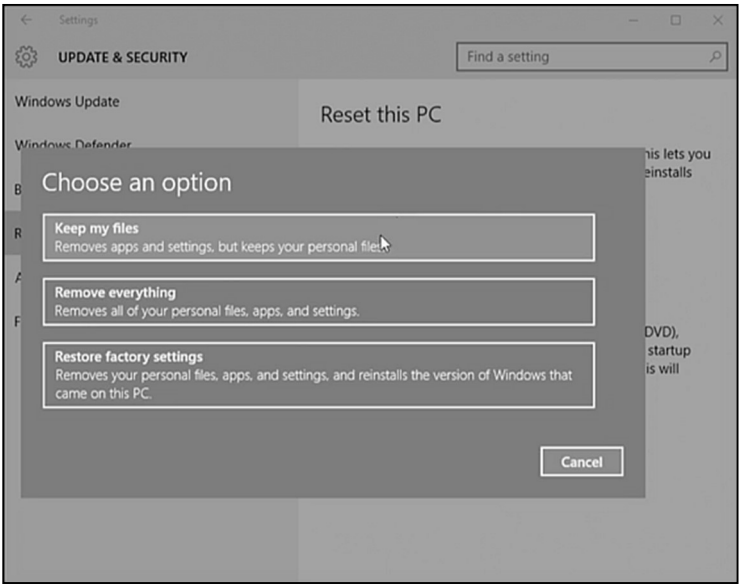
Dacă nu există un hard drive conectat, nu se alege *Add a drive*, ci *More options*, apoi se dă clic pe *Select a network location*, apoi pe *Add a network location* și se alege drive-ul din rețea, iar în final se apasă *OK* și *Turn on*.

Restaurarea fișierelor se fac cu: *Start – Settings – Update & Security – Backup – More options – Restore files from a current backup*. Se face deplasarea între backupuri cu *tastele săgeți*, se selectează *folderele* și *fișierele* dorite, apoi se dă clic pe *butonul verde*.

Funcţia Reset

Prin această funcţie se *reinstalează* Windows 10, *fără a afecta bibliotecile existente* sau cu *ştergerea definitivă* a acestora, în caz că doriţi să vindeţi computerul.

Se urmează calea: *Start – Settings – Update & Security – Recovery – Reset this PC – Get started*.



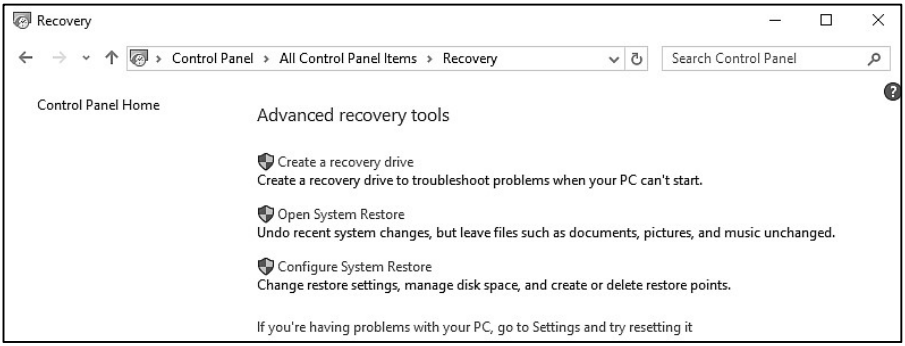
Aveţi la dispoziţie 3 opţiuni: *Keep my files* (aplicaţiile şi setările se pierd, dar rămân intacte bibliotecile personale), *Remove everything* (se pierde totul, iar computerul se vinde doar cu sistemul de operare) şi *Restore factory settings* (revenirea la versiunea cu care s-a achiziţionat computerul, pierzându-se aplicaţiile, setările şi bibliotecile personale).

Cea de-a treia opţiune nu va apărea la toate computerele pe care este instalat Windows 10. Deosebirea dintre ultimele două opţiuni nu este esenţială, dar este recomandabil să se aleagă ultima, atunci când aceasta este prezentă, deoarece permite şi refacerea unor *software-uri speciale* care însoţeau sistemul de operare atunci când a fost achiziţionat computerul.

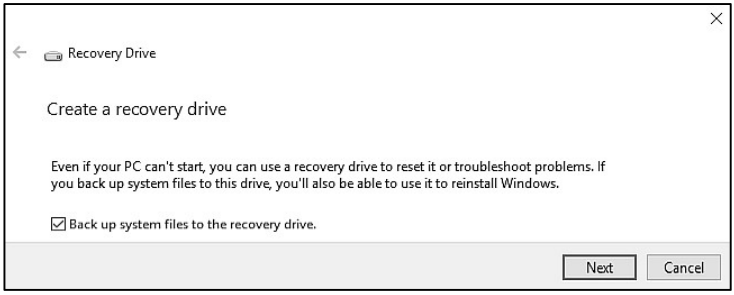
Funcția Recover

Dacă sistemul de operare nu mai bootează sau bootează incorect, se poate utiliza un drive USB pentru bootare, creat anterior cu funcția *Recover*.

Se introduce drive-ul USB și se urmează calea: clic drept pe *Start – Control Panel – All Control Panel Items – Recovery – Create a recovery drive*.



Apare fereastra următoare:



Asigurați-vă că ați bifat *Back up system files to the recovery drive*, apoi apăsați *Next*. Selectați drive-ul USB care apare disponibil și apăsați din nou *Next*, după care apăsați butonul *Create* pentru a porni crearea drive-ului bootabil. Acesta va fi formatat automat, așa că datele aflate pe acesta se vor pierde.

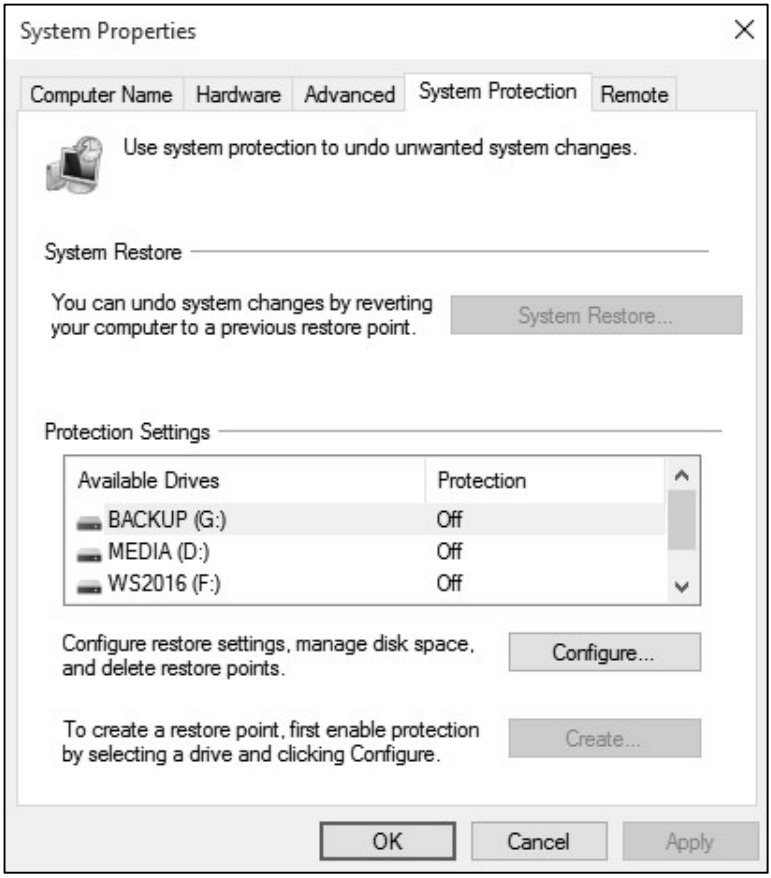
După o perioadă de timp de aproape o oră, apăsați *Finish* în fereastra finală.

Când aveți probleme la bootare, introduceți drive-ul în portul USB și bootați de pe acesta. Dați clic pe *Troubleshoot*, apoi pe *Recover from a drive*.

Punctele de restaurare

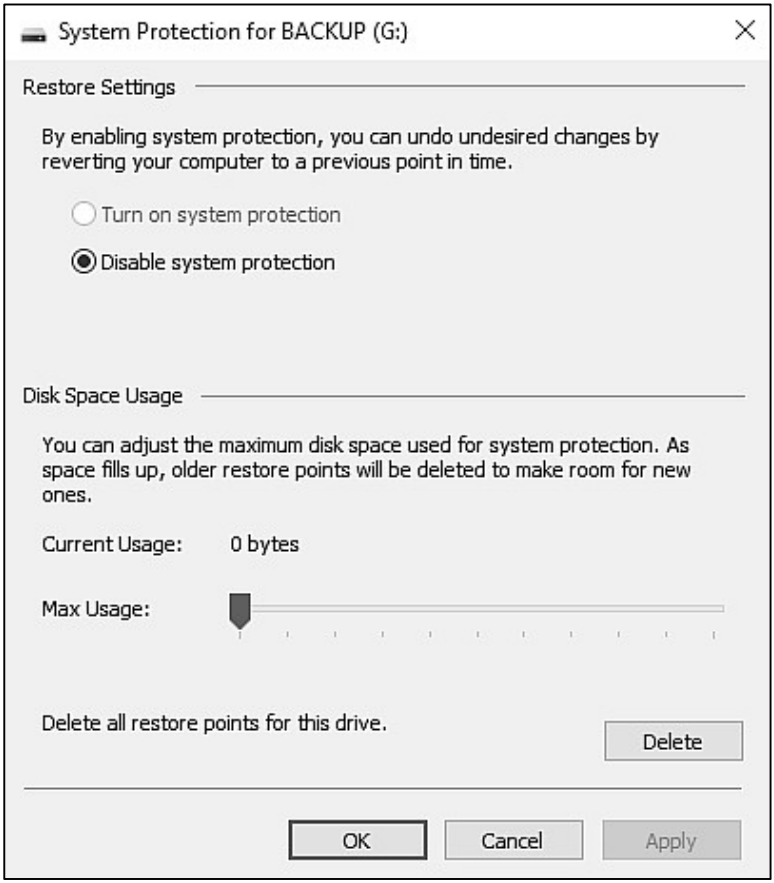
Rezolvarea problemelor legate de sistemul de operare se poate face și prin crearea punctelor de restaurare (*restore points*).

Deschideți *File Explorer* și dați clic drept pe *This PC*, apoi clic pe *Properties*. În partea din stânga sus a ferestrei care apare, dați clic pe *System Protection*.



Puteți apăsa butonul *Configure* pentru a activa sau dezactiva protecția sistem (*Turn on system protection, Disable system protection*), puteți stabili spațiul

necesar pentru punctul de restaurare (*Sisk Space Usage*) sau puteți șterge unul sau mai multe puncte de restaurare anterioare, apăsând butonul *Delete*.



Puteți crea manual un punct de restaurare, apăsând butonul *Create*, în fereastra *System Properties*. Introduceți numele punctului și apăsați *Create*.

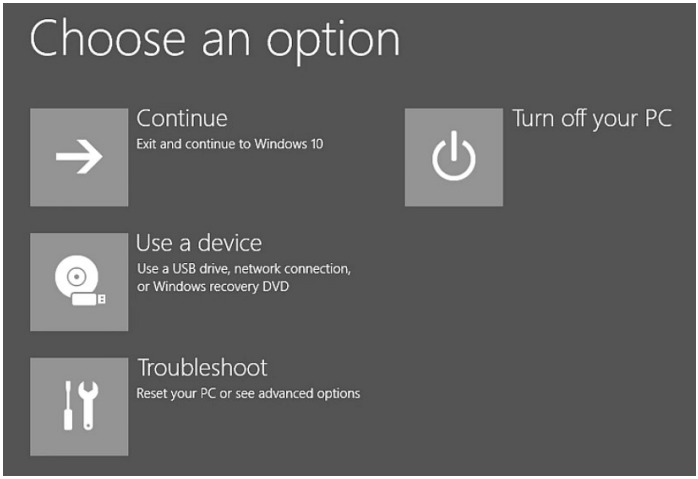
Pentru a readuce sistemul într-un punct de restaurare anterior, se apasă butonul *System Restore* din fereastra *System Properties*, apoi *Next*, se selectează punctul de restaurare dorit și se apasă succesiv butoanele *Next* și *Finish*.

Startup avansat

Există trei modalităţi de a afectua startup avansat:

1. *Start – Settings – Update & Security – Recovery – Restart now*
2. Clic drept pe *Start* – clic pe *Command Prompt (admin)*, apoi se introduce la prompter următoarea comandă:
 ...>*shutdown.exe /r /o*
3. *Start – Power – Shift + Restart*

În cazul nostru vom alege cea de-a treia metodă, care va duce la apariţia următorului panou:



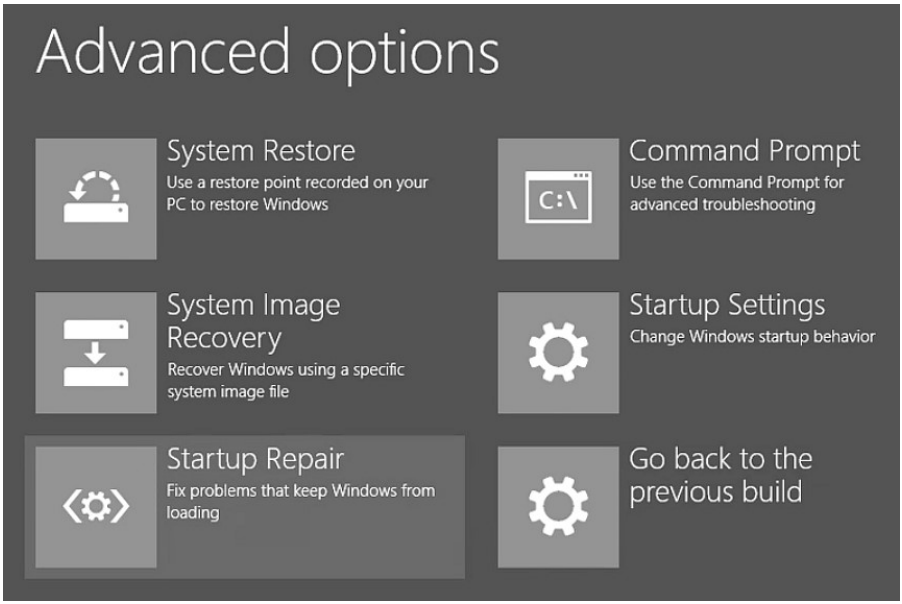
Apăsaţi butonul *Troubleshoot*, iar din următoarele două butoane alegeţi *Advanced options*. Apare o fereastră specială, cu mai multe opţiuni.

Prin *System Restore* se poate reveni la un punct de restaurare salvat anterior, când sistemul de operare funcţiona corect.

System Image Recovery ajută la refacerea sistemului de operare utilizând o imagine ISO a acestuia.

Problemele care apar la încărcarea sistemului de operare pot fi eliminate cu opţiunea *Startup Repair*.

Depanarea sistemului de operare se poate face şi tastând comenzi la prompter (*Command Prompt*).



Prin *Startup Settings* se poate schimba comportamentul sistemului de operare la bootare (schimbarea rezoluției display-ului, activarea modului depanare – *debugging mode,* activarea logării la bootare, intrarea în Safe Mode, dezactivarea semnăturilor driverelor, dezactivarea protecției malware *early-launch* sau dezactivarea restartării automate la întâlnirea unei erori de sistem de operare).

Opțiunea *Go back to the previous build* vă ajută se reveniți la versiunea anterioară a sistemului de operare.

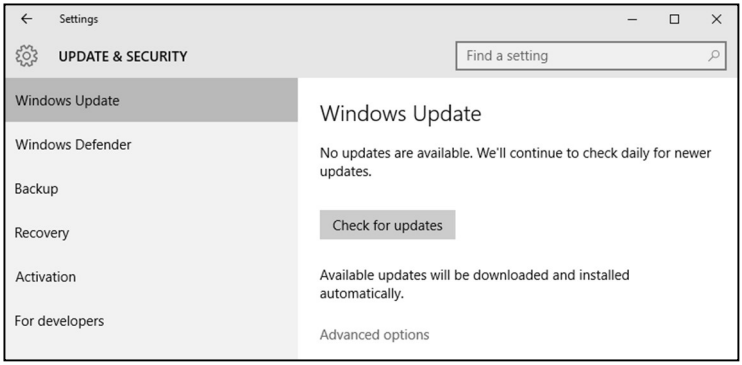
Update-uri uzuale și majore

Politica update-urilor în Windows 10

Windows 10 va fi ultima versiune de Windows lansată de Microsoft. În viitor vor exista doar actualizări (*update*-uri) ale lui Windows , care vor fi trimise periodic către utilizatori.

Acestea vor fi descărcate și instalate automat, dar este posibilă și o instalare manuală: *Start – Settings – Update & Security – Windows Update – Check for Updates – Install now*.

Actualizările *automate* vor fi efectuate în perioadele de inactivitate ale computerului, pentru a nu influența negativ conexiunea la Internet și performanțele acestuia.



Unii utilizatori preferă să *invalideze* actualizările automate, deoarece, de multe ori, în timpul unei astfel de actualizări, computerul poate deveni inacesibil.

Pentru a face posibil acest lucru, se selectează opțiunea *Advanced options*. În fereastra care apare se poate trece de la *Automatic (recommended*) la *Notify to schedule restart* (notificare pentru programare restart).

La apariția unei noi actualizări, utilizatorul va fi *avertizat* printr-un mesaj și va instala actualizarea doar atunci când va considera că este momentul potrivit.

Este important ca actualizările să se facă în timp util, deoarece multe dintre ele îmbunătățesc *securitatea* sistemului de operare și îl protejează împotriva atacurilor din exterior.

Trebuie precizat faptul că nu toate categoriile de utilizatori vor putea aplica aceeași *politică de update-uri* (acceparea, amânarea sau anularea update-urilor).

Există trei variante principale prin care update-urile de Windows 10 vor fi trimise către utilizatori: *Current Branch* (CB), *Current Branch for Business* (CBB) și *Long Term Servicing Branch* (LTSB).

Pentru utilizatorii de *Windows 10 Home* se va aplica politica *CB*. Toate noile facilități, patch-urile și update-urile vor fi trimise prin Windows Update. Politica CB nu permite amânarea sau anularea update-urile, acestea instalându-se în mod obligatoriu în momentul recepționării acestora.

Pentru utilizatori de *Windows 10 Pro* se va aplica politica *CBB*. Aceștia vor putea alege momentul instalării update-urilor, având posibilitatea de amânare pentru momentele în care computerul este mai liber.

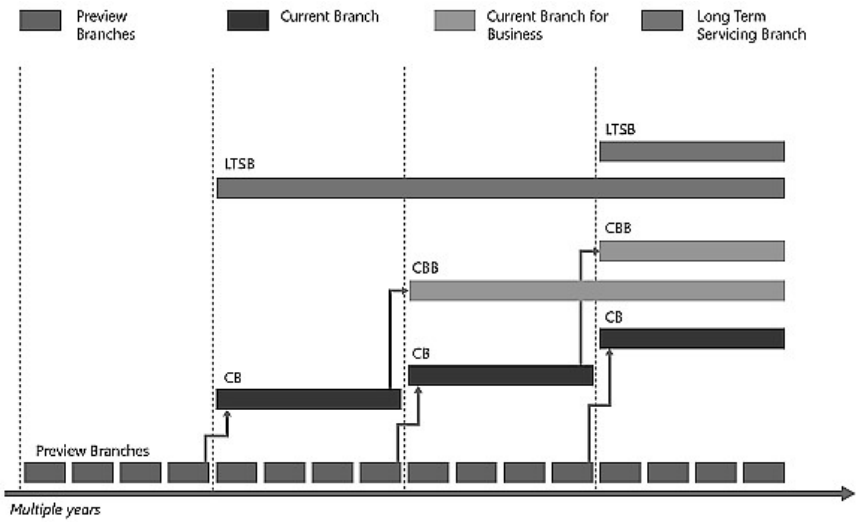
Totuși această amânare nu poate dura la infinit, utilizatorii de Windows 10 Pro fiind totuși obligați să instaleze update-urile în ordinea cronologică a emiterii acestora. Durata maximă de amânare este de 4 luni.

Utilizatorii *de Windows 10 Enterprise* și *Windows 10 Education* vor aplica politica *LTSB*, prin care pot alege doar update-urile de securitate, anulând update-urile care introduc noi facilități ale sistemului de operare. Aici durata maximă de amânare este de 12 luni.

Pentru celelalte categorii de utilizatori (*Windows 10 Mobile*, *Windows 10 Mobile Enterprise* și *Windows IoT*) se va aplica aceeași politică *CBB* ca la Windows 10 Pro.

Ediția de Windows 10	**Politica update-urilor**
Home	CB
Pro Mobile Mobile Enterprise IoT	CBB
Enterprise Education	LTSB

Există următoarele categorii de update-uri: *Servicing Updates* (Security features, Important updates, Patch Tuesday, Out-of-band) și *Feature Upgrades* (noi facilități). Lista tuturor update-urilor efectuate se poate vizualiza urmând calea: *Start – Settings – Update & Security – Windows Update – Advanced options – View your update history*.



Imagine preluată de pe *technet.microsoft.com*

Primul update major al lui Windows 10, *Redstone,* conține extensii pentru Microsoft Edge, îmbunătățiri pentru modul Continuum și alte noutăți. Data probabilă la care va fi disponibil va fi la un an după lansarea lui Windows 10, deci în jur de 1 august 2016. Redstone ar putea să aibă un impact similar trecerii de la Windows 8 la Windows 8.1.

Redstone 2, următorul update major, a fost amânat pentru 2017, din considerente hardware, pentru a coincide cu lansarea echipamentelor *Surface Pro 4* și *Surface Book*.

Observație

Dacă urmați calea *Start – Settings – Update & Security – Windows Update – Advanced Options – Choose how updates are delivered*, asigurați-vă că *Updates for more than one place* este pe poziția *Off*. Dacă acesta este pe *On* (implicit), atunci puteți primi update-uri și de la alte surse în afară de Microsoft, care pot periclita siguranța computerului dumneavoastră.

Licențiere

Moduri de licențiere

După cum am arătat în volumul anterior, „*Windows 10 Ghid practic*", pentru PC-uri, laptopuri și all-in-one există patru ediții ale lui Windows 10: *Home, Pro, Enterprise* și *Education*.

Doar de la *Windows 10 Pro* în sus se pot utiliza *introducerea în domeniu* și *politica de grup (Group Policy)* și doar la edițiile *Enterprise* și *Education* se pot utiliza *virtualizările* (Client Hyper-V) și alte *facilități* caracteristice computerelor care lucrează în rețele LAN (Device Guard, DirectAccess, AppLocker etc.).

Windows 10 IoT Core lucrează pe dispozitive ca *Rasberry Pi 2, MinnowBoard MAX, ATM-uri, GPS-uri manuale* sau chiar *telecomenzi* ale televizoarelor..

Licențierea gratuită pentru *Windows 10 Home* și *Pro* va fi posibilă doar până la 29 iulie 2016, pe sistemele care au instalate Windows 7, Windows 7 Pro, Windows 7 Ultimate, Windows 8.1 sau Windows 8.1 Pro cu licență.

Windows 10 Enterprise nu este disponibil pentru upgrade gratuit.

După 29 iulie 2016, licențele pentru oricare din cele șapte ediții ale lui Windows 10 (vezi „*Windows 10 Ghid practic*") se pot achiziționa doar contracost.

Pentru rețelele cu *mai puțin de 250 de utilizatori* ai lui Windows 10, Microsoft oferă trei tipuri de licențiere: *Open value* (include asigurări software)*, Open Value Subscription* (licențiere pe un singur an) și *Open License* (minimum 5 licențe).

Pentru rețelele cu mai mult de 250 de utilizatori există trei opțiuni: *Enterprise Agreement*, *Microsoft Product and Services Agreement- MPSA* și *Select Plus* (abandonată în iulie 2015).

Enterprise Agreement include *Tiered Priceing* (prețuri diferențiate) și *Software Assurance* (asigurare software) pe trei ani. De asemenea, include:

- *Professional Desktop Platform Enrollment: Windows Enterprise Upgrade, Office Professional Plus* și *Core CAL* (Exchange și SharePoint);
- *Enterprise Desktop Platform Enrollment: Windows Enterprise Upgrade, Office Professional Plus* și *Enterprise CAL* (Exchange, SharePoint și alte aplicații similare).

Software Assurance include *Upgrade Rights, Planning Services, Training Vouchers, Elearning* și *24x7 problem resolution suport*.

Pentru detalii suplimentare privind licențierea descărcați fișierul PDF intitulat *Volume Licensing Reference Guide for Windows 10* de pe site-ul *download.microsoft.com*.

Cuprins

Noutăți pentru profesioniști – 3

Configurare
Settings și Control Panel – 8
Control Panel propriu – 24
God Mode – 26
Start Menu identic pe toate computerele – 27
Controlul nivelului de acces al utilizatorului – 28
Action Center invizibil – 29
Redirectarea traficului de la Edge la Internet Explorer – 30
Registry Editor – 30

Securitate
Securitatea în Windows 10 – 32
Securizarea hardware – 35
Securizarea identităților – 39
Securizarea software – 45

Rețele
Îmbunătățiri aduse rețelelor wireless – 54
Wi-Fi Sense – 56
Conectarea prin VPN Wi-Fi – 57
Power Shell – 59
Remote Desktop - 60
Suport pentru IPv6 - 64

Virtualizare
Mașini virtuale – 66
Client Hyper-V – 67
Virtualizarea desktop-urilor – 74
Virtualizarea aplicațiilor – 75
Virtualizarea drive-urilor – 76
UE-V – 80

Configurarea și securizarea datelor
Managementul spațiului ocupat pe drive-uri – 82
OneDrive – 86
OneDrive for Bussines – 89
Autorizarea accesului la date – 90
Convertirea drive-urilor și partițiilor la NTFS – 95
Enterprise Data Protection – 97
Encripted File System - 99
BitLocker – 101

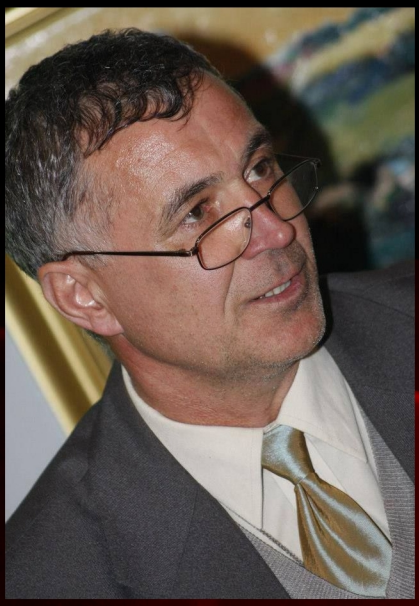
Partajarea resurselor
Partajarea imprimantelor – 106
Partajarea cu HomeGroups – 109
Partajarea folderelor și fișierelor – 112

Managementul accesului la date
Alocarea spațiului de drive-uri și partiții – 118
Managementul folderelor cu File Explorer – 121
Utilizarea bibliotecilor – 126
Redirecționarea bibliotecilor – 128
Auditul folderelor și fișierelor – 131

Salvare și restaurare
Backup și Restore – 136
File History – 138
Funcția Reset – 139
Funcția Recover – 140
Punctele de restaurare – 141
Startup avansat – 143

Update-uri uzuale și majore
Politica update-urilor în Windows 10 – 146

Licențiere
Moduri de licențiere – 150



Nicolae Zărnescu a absolvit Liceul de Informatică (actualul Colegiu Național de Informatică „Tudor Vianu”) și Facultatea de Automatică și Calculatoare, din cadrul Universității Politehnice, ambele în București.

A lucrat ca programator în limbajele Z80, Fortran, Cobol, Pascal, Visual Basic, dBase și Fox și ca inginer de sistem pentru rețele Novell și Windows Server.

Cărțile sale de referință se numesc ***Pașaport pentru lumea de dincolo*** (o îmbinare a ezoterismului cu fizica modernă), ***Ghid practic de fotografie digitală*** (cea mai actuală carte de acest gen din România) și ***WINDOWS 10 Ghid practic*** (prima carte în limba română despre noul sistem de operare)

WINDOWS 10 pentru profesioniști prezintă, în detaliu, cea mai reușită versiune de Windows creată vreodată de Microsoft.